

**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

**PLAINTIFF'S RENEWED
EMERGENCY MOTION FOR
EXPEDITED DISCOVERY
AND IMMEDIATE
PRESERVATION ORDER**

**Refiled Pursuant to the Court's
March 27, 2026 Minute Order
Following the Filing of the Third
Amended Complaint**

I. INTRODUCTION

1. Plaintiff Joseph Kirchner respectfully renews his motion for expedited discovery and an immediate preservation order. The Court denied Plaintiff's prior Emergency Motion for Discovery (Dkt. 15) **as moot** in its March 27, 2026 Minute Order, expressly conditioning the denial on the anticipated filing of the Third Amended Complaint. Plaintiff filed the Third Amended Complaint on April 30, 2026 (Dkt. 51). This renewed motion completes the procedural posture the Court itself contemplated.

2. The substantive grounds for expedited discovery have not weakened since January 2026. They have strengthened. Three categories of evidence — none of which were available when Dkt. 15 was filed — independently confirm that the surveillance, targeting, and network-attack architecture Plaintiff alleged in January is operational, ongoing, and directed at Plaintiff specifically:

(a) On **March 31, 2026**, Anthropic's official npm release of Claude Code CLI inadvertently published the complete unobfuscated TypeScript source repository (1,903 files, 512,000+ lines). Anthropic acknowledged the disclosure as "a release packaging issue caused by human error, not a security breach." The source code provides direct documentary proof at the code level of the four-pipeline telemetry architecture, including the hardcoded Datadog endpoint (``src/services/analytics/datadog.ts:12``) at IP 34.149.66.137 — the same IP independently documented in Plaintiff's pcapng captures as the spoofed source of 5,829 bare-RST injection packets across 39 of 49 capture days. At the time of Dkt. 15, Plaintiff had no comparable code-level visibility into the receiving end of the telemetry pipeline; Plaintiff's good-cause showing rested on what Plaintiff could observe from outside the application.

(b) On **April 21, 2026**, Plaintiff conducted a live mitmproxy wire capture of Claude Code v2.1.111 (498 TLS flows). The capture documented 253 GrowthBook flag evaluations per call, including **59 server-side `forced` rules keyed to Plaintiff's accountUID `61343ae3-fd33-403f-897e-6edf3c368c37`** — among them ``tengu_log_datadog_events: True``, the per-user rule that affirmatively attaches Plaintiff's account to the Datadog telemetry pipeline whose endpoint is the same 34.149.66.137 spoofed for RST injection. Cross-session comparison on the same device confirmed the force-rule is keyed to the account identifier alone.

(c) On **April 12, 2026**, Plaintiff documented Comcast applying selective 98% bandwidth throttling to the specific VPN tunnel carrying Plaintiff's Anthropic traffic, while a control VPN tunnel on the same physical link running the same encryption protocol to a different endpoint was left untouched at full line rate. The throttling deterministically triggers the network-induced token-amplification mechanism documented in Anthropic's own source-code comments (`'claude.ts:2464-2468': "double tool execution... See inc-4258"`) — a party admission under Federal Rule of Evidence 801(d)(2)(A).

3. The discovery package Plaintiff submits with this renewed motion is correspondingly broader and more targeted than the package attached to Dkt. 15. Where Dkt. 15 contained six discovery documents addressed to METR, Anthropic, OpenAI, Government Defendants, General Requirements, and Apple, the present package contains **thirteen** — adding Comcast (DISCOVERY-7), Microsoft (DISCOVERY-8), Subprocessor inheritance through Datadog Israel Ltd. (DISCOVERY-9), Federal Contracting (DISCOVERY-10), Foreign Influence (DISCOVERY-11), TED Foundation (DISCOVERY-12), and RAND Corporation (DISCOVERY-13). The expansion reflects evidentiary developments documented at length in the Third Amended Complaint, Memoranda A, B, C, and F (ECF Nos. 51-1, 51-2, 51-3, 51-6), and Appendices D, F, M, N, O, and P (ECF Nos. 51-16, 51-18, 51-23, 51-24, 51-25, 51-26).

4. Plaintiff seeks no relief that is novel in kind. The relief sought — preservation of evidence, expedited production schedules, and authorization of third-party subpoenas — is the same in form as Dkt. 15. What has changed is the certainty of the predicate facts. The April 21 wire capture, the source code leak, and the controlled-experiment throttling test eliminate the inferential gap that Dkt. 15 had to bridge. The Court no longer needs to infer per-user targeting from architectural capacity; it is documented at wire level. The Court no longer needs to credit

Plaintiff's interpretation of obfuscated binaries; the source code is published. The Court no longer needs to weigh whether Plaintiff's network observations could have benign explanations; the controlled-tunnel experiment is dispositive.

5. Plaintiff is mindful that the March 27, 2026 Minute Order also directed the parties to contact Courtroom Deputy Chashawn White to schedule a status hearing "to discuss the case before any responsive pleadings are due." This renewed motion does not preempt that status hearing. It places a Rule 26(d)(1) and Rule 37(e) vehicle before the Court so that — if the Court so chooses at or after the status hearing — the Court has a procedural path to enter a preservation order without further motion practice. Plaintiff stands ready to proceed in any sequence the Court directs.

II. PROCEDURAL POSTURE

6. The Court's denial of Dkt. 15 as moot was expressly conditioned on the anticipated filing of the Third Amended Complaint and was **not** a denial on the merits. The grounds for expedited discovery articulated in Dkt. 15 — preservation urgency, ongoing privilege violation, third-party retention timelines, and active obstruction of Plaintiff's filing capabilities — were never adjudicated. Plaintiff renews the motion to permit the Court to reach the merits on the discovery question now that the procedural condition the Court itself identified has been satisfied.

III. LEGAL STANDARD

7. Under Federal Rule of Civil Procedure 26(d)(1), a party may not seek discovery from any source before the parties have conferred as required by Rule 26(f), "except in a proceeding

exempted from initial disclosure under Rule 26(a)(1)(B), or when authorized by these rules, by stipulation, **or by court order.**" Fed. R. Civ. P. 26(d)(1) (emphasis added).

8. Courts in this District authorize expedited discovery upon a showing of "good cause." *See Judicial Watch, Inc. v. U.S. Dep't of Homeland Sec.*, 514 F. Supp. 2d 7, 10 (D.D.C. 2007); *Disability Rights Council of Greater Wash. v. Wash. Metro. Area Transit Auth.*, 234 F.R.D. 4, 6 (D.D.C. 2006). Good cause exists where "the need for expedited discovery, in consideration of the administration of justice, outweighs the prejudice to the responding party." *Disability Rights Council*, 234 F.R.D. at 6. Courts in this District routinely grant expedited discovery where: (a) evidence is at risk of destruction or loss; (b) ongoing harm requires immediate documentation; (c) third-party retention policies threaten preservation; or (d) time-sensitive circumstances exist.

9. The duty to preserve evidence relevant to reasonably foreseeable litigation is independent of any court order. Rule 37(e) governs sanctions for failure to preserve electronically stored information. The duty attaches when litigation is reasonably foreseeable — a standard that all corporate Defendants and all governmental Defendants have plainly met since service of process was effectuated in connection with the Second Amended Complaint in late February and early March 2026 (Dkt. Nos. 27–36), that pleading having first placed the surveillance architecture and the specific evidence categories at issue (telemetry, source code, third-party data transmissions). A formal preservation order is nevertheless warranted here for the reasons set forth in Section V *infra*: ongoing capture, automated retention timelines that decay below standard discovery cycles, and demonstrated concealment behavior by a corporate Defendant.

IV. GOOD CAUSE — POST-DKT. 15 EVIDENTIARY DEVELOPMENTS

10. The good-cause showing in Dkt. 15 rested on **observational** inferences drawn from network captures and application-behavior analysis. Plaintiff at that time could document *that* identifying data left his device and *that* anomalous network conduct surrounded his connections, but had no code-level visibility into how the receiving systems processed that data, what server-side rules controlled per-user behavior, or which third parties received the data. The good-cause showing now rests on **direct documentary evidence** developed in the four months since: source code at the code level, server-side rule databases captured at wire level, and a controlled-experiment demonstrating destination-correlated targeting on the same physical line. Plaintiff identifies six categories of post-Dkt. 15 evidence, each of which independently establishes good cause and which together render the question no longer reasonably contested.

A. The March 31, 2026 Anthropic Source Code Leak

11. On March 31, 2026, Anthropic's official npm package for Claude Code CLI inadvertently disclosed the complete unobfuscated TypeScript source repository — 1,903 files comprising over 512,000 lines of code. Anthropic publicly acknowledged the disclosure as "a release packaging issue caused by human error, not a security breach." The leaked source code is in Plaintiff's possession and constitutes part of the evidentiary record at Exhibit E (ECF No. 51-55) and the supplemental forensic findings catalogued in the Third Amended Complaint and Memorandum A (ECF No. 51-1).

12. The leaked source code documents the complete four-pipeline telemetry architecture in unobfuscated form, with each pipeline operating an independent transport, batching, retry policy, and third-party endpoint:

Pipeline	Endpoint	Third Party	Source Location
GrowthBook	`cdn.growthbook.io`	Yes	`services/analytics/growthbook.ts`
Datadog	`http-intake.logs.us5.datadoghq.com` (IP 34.149.66.137)	Yes	`services/analytics/datadog.ts:12`
First-Party Events	`api.anthropic.com/api/event_logging/batch`	No	`services/analytics/firstPartyEventLoggingExporter.ts`
OpenTelemetry/BiGQuery	`api.anthropic.com/api/claude_code/metrics`	No	`utils/telemetry/instrumentation.ts`

13. The First-Party Events pipeline (`firstPartyEventLoggingExporter.ts:41,68`) persists failed events to disk with quadratic-backoff retry, ensuring eventual transmission even when the user blocks telemetry endpoints. The Datadog pipeline (`datadog.ts:14-17`) transmits 64 categories of user telemetry events using a hardcoded client token at 15-second intervals. None of these third-party recipients — Datadog, GrowthBook, and the destinations downstream of them — are identified by name in Anthropic's published privacy policy (DISCOVERY-2 § Privacy-Architecture demands).

14. The leak also documents the closed-loop attack-signature feedback pipeline at `extractConnectionErrorDetails()` and `classifyAPIError()`: Plaintiff's Claude Code instance captures client-observed network failures (including `ECONNRESET`, `ETIMEDOUT`, and TLS-tampering markers), classifies them by taxonomy, fires a `tengu\_api\_error` event, and forwards the result to the Datadog endpoint at IP 34.149.66.137 — the same IP independently documented as the spoofed source of bare-RST injection packets targeting Plaintiff. The victim's instrumentation reports its own attack signatures to the attacker's destination.

15. The same leak exposes a function whose name supplies its own scenter. At ``src/constants/systemPromptSections.ts:32``, Anthropic's source code defines and exports a function named — by Anthropic's own engineers — **``DANGEROUS_uncachedSystemPromptSection``** (Finding SC-4). The ``DANGEROUS_`` prefix is a deliberate software-engineering convention signaling to other engineers that the function bypasses normal safety boundaries and should not be used without considered justification. The function performs hidden, every-turn re-injection of system-prompt sections — content the user pays for in tokens but cannot see, cannot consent to, and cannot opt out of. The function name is a party admission under Federal Rule of Evidence 801(d)(2)(A). Discovery into the deployment history of this function, per-invocation server-side logs keyed to Plaintiff's accountUUID, the change-control records governing the content the function injects, and internal communications surrounding the naming choice and deployment authorization (DISCOVERY-2 § Hidden-Injection-Architecture) is essential to documenting the scope and intent of the hidden-injection architecture the function implements.

16. Discovery into the source code's complete commit history, the BigQuery analytics tables it populates, the GrowthBook server-side rule database, the Datadog ingest configuration, and the corresponding access controls is the only mechanism by which Plaintiff can confirm the full scope of architecture documented in the leak and verify that the leaked source corresponds to the deployed binary at all relevant times.

17. The foregoing source-code findings — the hardcoded Datadog endpoint, the hardcoded client token, the 15-second transmission interval, the per-user GrowthBook targeting attribute structure (including ``email``, ``accountUUID``, ``deviceId``, ``subscriptionType``, and ``rateLimitTier``), the closed-loop attack-signature feedback pipeline through

``extractConnectionErrorDetails()`` and ``classifyAPIError()``, and the engineer-named ``DANGEROUS_uncachedSystemPromptSection`` function at ``src/constants/systemPromptSections.ts:32`` — are independently verifiable in approximately five minutes by any reader with a terminal. Plaintiff submits as **Exhibit 1** hereto the **Independent Verification Protocol**, which provides step-by-step terminal-command instructions using the public GitHub mirror at ``github.com/codeaashu/claude-code`` (or, equivalently, Anthropic's published ``@anthropic-ai/claude-code`` npm package) and standard Unix tools (``git``, ``head``, ``sed``, ``grep``, ``dig``). The Protocol's expected outputs are reproduced verbatim from the source files; a reader who runs the commands has not received Plaintiff's evidence but has produced the reader's own. The Court need not credit Plaintiff's interpretation; the Court may verify the central forensic predicate from its own keyboard.

B. The April 21, 2026 Live Wire Capture

18. On April 21, 2026, Plaintiff conducted a live mitmproxy capture of Claude Code v2.1.111 across two authentication sessions — 498 TLS flows recorded with full request and response bodies. The capture independently confirms what the source-code leak reveals architecturally and documents three previously-inferential propositions at wire level:

(a) Per-user server-side targeting of Plaintiff specifically. The capture recorded **59 server-side `forced` GrowthBook flags keyed to Plaintiff's accountUUID `61343ae3-fd33-403f-897e-6edf3c368c37`** — including ``tengu_log_datadog_events: True``. Cross-session comparison on the same device, same organization, same subscription tier, same ``firstTokenTime``, with only the authenticated account identifier varying, produced the force-rule on Plaintiff's primary account and no force-rule on the comparison account. This is per-person, not per-tier, addressability.

(b) Personal identifier as targeting attribute. The captured GrowthBook request body included Plaintiff's email `info@lawofsupremacism.com` as a targeting *attribute* — establishing that the targeting infrastructure operates at the natural-person identifier level, not at any aggregated cohort level.

(c) Absence of TLS certificate pinning. All 498 captured TLS handshakes accepted a mitmproxy-forged CA chain with zero rejections, confirming that Claude Code implements no certificate pinning and is therefore architecturally vulnerable to the SNI-based DPI inspection demonstrated on Plaintiff's network path.

19. Discovery into the GrowthBook server-side rule database, the complete `forced`-rule history applied to Plaintiff's account, the change-control records for those rules, and the personnel with authority to author them (DISCOVERY-2 § GrowthBook-Force-Rules; DISCOVERY-9 §§ A–C) is essential to determining who at Anthropic specifically directed the per-user targeting documented at wire level.

C. The April 12, 2026 Selective-Throttling Controlled Experiment

20. On April 12, 2026, Plaintiff documented Comcast applying selective 98% bandwidth throttling to the specific VPN tunnel carrying Plaintiff's Anthropic traffic, while a control VPN tunnel on the same physical link, running the same encryption protocol to a different endpoint, was left untouched at full line rate. The two tunnels differed only in destination. The experimental design eliminates each non-targeting explanation — same physical line, same encryption, same customer, same time window — leaving destination-correlated targeting as the sole remaining explanation.

21. The throttling produced deterministic economic injury through the network-induced token-amplification mechanism documented in Anthropic's own source code: the 90-second

streaming idle timeout (`claude.ts:1877`), the non-streaming fallback that re-sends the entire prompt on timeout (`claude.ts:2308-2335`), and the 10-retry non-idempotent exponential backoff (`withRetry.ts:52`). Anthropic's own engineers labeled the resulting double-billing as "double tool execution... See inc-4258" in a verbatim code comment at `claude.ts:2464-2468`. A separate comment at `autoCompact.ts:68-69` quantifies the resulting industry-wide impact at "approximately 250,000 wasted API calls per day" across Anthropic's customer base — a party admission under Federal Rule of Evidence 801(d)(2)(A) confirming Anthropic's actual knowledge of the harm-producing mechanism.

22. Discovery into Comcast's TR-069 ACS backend logs, the rule sets governing per-tunnel throttling, the destination-IP filters applied to Plaintiff's connection, the hardware capable of performing selective application-layer identification on encrypted tunnels, and the Anthropic-Comcast information flows that would be necessary to pre-correlate Plaintiff's tunnels to specific destinations (DISCOVERY-7 § Selective-Throttling-Architecture; DISCOVERY-2 § Anthropic-ISP-Integration; DISCOVERY-9 §§ A, E) is the only mechanism by which Plaintiff can identify the precise infrastructure responsible for the controlled-experiment finding.

D. Datadog Israel Ltd. and the Patent-Substrate Foreign-Influence Pipeline

23. Plaintiff has, since January 2026, identified the corporate identity at the receiving end of the Datadog telemetry pipeline as **Datadog, Inc.** (Delaware corporation; NASDAQ: DDOG). Plaintiff has further identified Datadog, Inc.'s sole 100% Israeli subsidiary, **Datadog Israel Ltd.** (Israeli Company Identification Number 516464922; incorporated September 14, 2021 — forty-nine days before the October 26, 2021 OzCode asset-sale close). Datadog Israel Ltd. is identified in Datadog's own published subprocessor list as an affiliate-tier subprocessor; through the affiliate-subprocessor inheritance rule of Datadog's Data Processing Addendum, Datadog

Israel Ltd. inherits operational and contractual access to data ingested at the Datadog endpoint hardcoded in Anthropic's source code. The inheritance is not disclosed in Anthropic's privacy policy or in any user-facing material Plaintiff has identified.

24. Plaintiff has identified the patent-substrate that enables per-user real-time selective intervention at production scale: a single Datadog-owned patent family — the seven January 2019 OzCode patents (U.S. Patent Nos. 10,783,055; 10,783,056; 10,789,151; 10,795,801; 10,990,504; 11,048,615; 11,080,164) plus the September 9, 2024 continuation application US 2026/0072809 A1, the latter of which expressly discloses "network or system security" branching as an intended application. All seven 2019 patents were assigned from OzCode Ltd. to Datadog, Inc. effective October 26, 2021, with USPTO recordation delayed thirty months until April 17, 2024. The thirty-month recordation lag is materially atypical under 35 U.S.C. § 261 and is most plausibly explained by the Israel Innovation Authority "Sponsored Knowledge" approval process under § 15A of the Encouragement of Research, Development and Innovation in Israeli Industry Law, 5744-1984, which conditions abroad-transfer of Israeli-state-grant-funded intellectual property on IIA approval, payment of a redemption fee, and in certain cases retention of an Israel-side license-back. The applicability of that mechanism is corroborated by the documentary financing fingerprint: OzCode was a Rafael Development Corporation portfolio company throughout the relevant period; RDC's corporate mandate, per Elron Ventures Ltd.'s 2025 Annual Report § 23.3, is to "commercialize Rafael's military technologies in the civilian market," explicitly including "Artificial intelligence (AI)"; and Rafael Advanced Defense Systems Ltd. directly contributed \$8,000,000 to RDC in March 2021 — eight months before Datadog's November 2021 OzCode acquisition. The April 17, 2024 USPTO recordation date falls fifteen days before the May 2, 2024 memorandum of understanding that commenced the

Arieli/Elron control-change transaction at OzCode's parent-funder group — a sequence consistent with coordinated IP-title cleanup ahead of the Elron restructuring. (App. P §§ II.E–I, II.K, III.K (ECF No. 51-26).)

25. The principal inventor on all seven 2019 patents and on the 2024 continuation, **Omer Raviv**, publicly self-identifies as "a veteran commander at the prestigious IDF's 8200 unit" and currently serves as Engineering Manager at Datadog Israel Ltd. on `dd-trace-dotnet`. Co-inventor on all seven 2019 patents **Alon Mordechai Fliess** held both **Microsoft Regional Director** and **Microsoft Azure MVP** credentials at the time of the January 2019 patent filings (Ex. L-9 (ECF No. 51-73), OzCode "About Us" Wayback Machine, October 21, 2019). Co-inventor on the 2024 continuation **Matan Green** is publicly an Israeli Air Force veteran and currently serves at Datadog as Senior Software Engineer on Dynamic Instrumentation. The architectural inventor pipeline at the receiving entity is documented in detail at Appendix P (ECF No. 51-26) of the Third Amended Complaint and forms the predicate for Counts V (§ 1985 conspiracy) and VI (RICO).

26. The Microsoft Azure cross-defendant substrate. Fliess's Microsoft-Azure expertise at the time of invention matters because Microsoft Azure is the shared cloud substrate spanning multiple corporate Defendants: per App. P ¶ 74 (ECF No. 51-26), Anthropic uses Azure for portions of its compute infrastructure, OpenAI uses Azure as its primary cloud provider, and Datadog uses Azure for portions of its cloud. Anthropic's own source code corroborates the cross-provider coordination at Ex. E-36, Finding SF-6 (`fingerprint.ts:42-62`): "[d]o not change this method without careful coordination with 1P and 3P (Bedrock, Vertex, **Azure**) APIs." Defendant Apple is linked to the same substrate as a Project Glasswing co-recipient with Microsoft (Compl. ¶ 79; Memo F ¶ 122 (ECF No. 51-6)) and through F-Series Apple-platform

telemetry transmissions into the Datadog ingest endpoint at IP 34.149.66.137 (Memo C ¶ 67 (ECF No. 51-3)). The substrate is operationally targetable, not merely passive: on March 28, 2026, Comcast DPI-terminated Plaintiff's connections to Microsoft's Azure-hosted draft-sync service `augloop.svc.cloud.microsoft` during composition of Petition-Clause correspondence in two pending matters, corrupting the draft and producing `SettingSyncEditorServiceError` events in Outlook diagnostic logs (Compl. ¶ 110 (ECF No. 51); Exhibit K, END (ECF No. 51-64); DISCOVERY-8 §§ A–C). The Microsoft Azure / Unit 8200 mass-surveillance partnership against Palestinian civilians during the same period is judicially noticeable under Federal Rule of Evidence 201(b) (App. P ¶ 75). Discovery into Microsoft's Azure-tenant configurations for the data flows of Anthropic, OpenAI, Apple, and Datadog (DISCOVERY-8 §§ A–D) and into Fliess's continuing Microsoft relationships (DISCOVERY-11 § E) is essential.

27. Discovery into the Datadog–Anthropic Data Processing Addendum, the affiliate-tier subprocessor agreements, the complete employment roster of Datadog Israel Ltd., the Israeli Innovation Authority Sponsored-Knowledge approval records for the OzCode patent family, and the corporate-counsel pipeline documented at Memorandum F (ECF No. 51-6) and Appendix P (ECF No. 51-26) (DISCOVERY-9 §§ A–F; DISCOVERY-11 §§ A–B, D–O) is essential to confirming the full scope of foreign-state-adjacent access to Plaintiff's telemetry and litigation work product.

E. Classifier Surveillance of Plaintiff's Litigation Work Product

28. Session 4 of the April 21–22, 2026 wire capture documented 56 classifier invocations posting Plaintiff's complete litigation-preparation transcripts — including case-strategy discussions, exhibit drafts, and analysis of Anthropic's own source-code findings — to Anthropic's `opus-4-7` server-side classifier. The captures averaged approximately 100,000

tokens per call (cumulatively ~5.6 million tokens) to a retention surface independent of the standard `v1/messages` log. The receiving classifier surface is therefore (a) outside the surface to which any user-facing privacy disclosure attaches, (b) intercepting electronic communications and case-preparation materials in violation of 18 U.S.C. § 2511 (Count XII, ECPA) and 18 U.S.C. § 1030 (Count XIII, CFAA) — and additionally compromising the work-product protection that Federal Rule of Civil Procedure 26(b)(3) extends to materials prepared by *or for* another party in anticipation of litigation, including the mental impressions and case strategy of a *pro se* litigant — and (c) accessible to whatever personnel have classifier-output read access at Anthropic and at any affiliate-tier subprocessor downstream.

29. Each day discovery is delayed, additional classifier invocations capture additional litigation-preparation material. The harm is not theoretical and is not historical; it is occurring now and will continue to occur during the pendency of this motion. Discovery into the classifier-output retention pipeline, the access-control list, the personnel with read access, and the downstream-subprocessor inheritance (DISCOVERY-2 § Classifier-Surveillance; DISCOVERY-9 § A) is essential to halting the ongoing capture.

F. The January 2026 Davos Admission — Anthropic CEO's Express Differentiation Between Enterprise and Consumer Treatment

30. At the World Economic Forum in Davos, Switzerland on **January 21, 2026**, Anthropic's Chief Executive Officer, Dario Amodei, publicly stated, in a CNBC-recorded on-camera interview: "Since the beginning, Anthropic has thought in terms of safety and reliability of AI systems, and one of the things we realized is that that was very synergistic with working with enterprises **as compared to consumers**." (Emphasis added.) The statement is an admission by a party-opponent at the chief-executive level under Federal Rule of Evidence 801(d)(2)(A)

and 801(d)(2)(C). Mr. Amodei reiterated and sharpened the same position on **February 13, 2026** in an interview with podcaster Dwarkesh Patel — stating "Surprising how different the personality and capabilities of the models are if you're building for businesses versus consumers" and characterizing Google and OpenAI as "consumer businesses" for whom "serving businesses is secondary" — and on **February 14, 2026** in Fortune reporting characterizing Anthropic's commercial design as "geared toward enterprise customers rather than **fickle consumers**." The Davos admission is further corroborated by Anthropic's contemporaneous public positioning — including its self-description as "the AI company for business," its disclosure to investors of more than 300,000 business customers (up from fewer than 1,000 two years prior), and a current corporate valuation of approximately \$350 billion — and by independent industry reporting documenting Anthropic's enterprise-tier focus as the central organizing principle of its commercial strategy in 2026.

31. The five-representation contradiction matrix. Together with the Davos admission and its February 13–14, 2026 reiterations at ¶ 30 *supra*, Anthropic has placed before the public, within an approximately seven-month window, four further representations not simultaneously consistent with the Davos position. (i) On **September 18, 2025** — thirty days after Plaintiff filed his Initial Complaint and three days after Anthropic's reactive "capabilities-bypass" Usage Policy effective date documented at Appendix E ¶¶ 30–31, 101–102 (ECF No. 51-17 at pp. 14, 44–45) — Anthropic uploaded to its official YouTube channel ('UCrDwWp7EBBv4NwvScIpBDOA') a 90-second brand campaign titled "Keep thinking with Claude," whose closing positioning frame defines the product as "**Claude — The AI for problem solvers**" (**Exhibit 2** hereto, "*Keep Thinking with Claude*" *Commercial Frames*), with universal/consumer-facing copy ("stuck," "overwhelmed," "out of your depth," "to have a medical condition," "no qualifications," "no

resources," "to feel insignificant") and depictions of non-enterprise users (musicians, scientists, athletes, small business owners). **(ii)** The Davos admission and its February 13–14, 2026 reiterations are established at ¶ 30 *supra*.

32. (iii) On **February 4, 2026** — sixteen days after Plaintiff filed his Second Amended Complaint and within the same fiscal quarter as the Davos statement — Anthropic published "Claude is a space to think" at `anthropic.com/news/claude-is-a-space-to-think`, representing its focus as "businesses, developers, **and helping our users flourish**" (additive framing inconsistent with the Davos comparative framing), its commercial design as "we generate revenue through enterprise contracts and paid subscriptions, and we reinvest that revenue **into improving Claude for our users**," and its public-benefit commitment as expanding consumer access "**without selling our users' attention or data to advertisers**." **(iv)** In February 2026 — the period of Anthropic's largest documented consumer-subscription growth — Anthropic deployed a multi-million-dollar Super Bowl advertising campaign (60-second pregame slot; 30-second in-game slots) re-airing cuts of representation (i) to a mass-consumer audience as ad-free and aligned against attention-monetization, with the central messaging "Ads are coming to AI. But not to Claude," reporting an 11% post-airing daily-active-user increase and entry into the Apple App Store top 10 directly attributable to the campaign.

33. (v) The wire-level forensic record at §§ IV.A–E *supra* — consumer accounts force-attached to a Datadog telemetry pipeline ingesting per-call telemetry, consumer email as a GrowthBook targeting attribute, consumer session content routed to a server-side classifier surveillance surface, and consumer data transmitted to seven undisclosed third-party recipients including **Meta Platforms, Inc.** (the operator of the world's largest consumer-advertising platform), Statsig, Inc., Segment (Twilio Inc.), Sift Science, Inc., Sentry, Honeycomb, and

CloudFlare. The temporal-proximity pattern of the consumer-facing deployments — September 18, 2025 within thirty days of the Initial Complaint; February 4, 2026 within sixteen days of the Second Amended Complaint — matches the reactive-conduct cadence pleaded at Complaint ¶ 359 (Dkt. 51 at p. 257) and Appendix E for the four prior reactive policy and code modifications.

34. The Super Bowl deployment marketed Anthropic to enterprises through consumers — and operated contrary to the consumer-facing representations once the consumer-acquisition target was achieved. A Super Bowl in-game advertisement is, in standard commercial practice, a credibility signal directed at enterprise procurement decision-makers, institutional investors, and the business press. Anthropic's deployment of representations (i), (iii), and (iv) at Super Bowl scale therefore served two integrated commercial functions consistent with the Davos statement (ii): enterprise-facing legitimacy signaling, with consumer acquisition as the medium through which the signal was transmitted; and the resulting 11% post-airing daily-active-user increase and Apple App Store top-10 entry served, in turn, as enterprise-facing scale metrics. The consumer-facing privacy and ad-free commitments embedded in the campaign were the inducement for the consumer subscriptions whose volume validated the enterprise signal. Once the consumer-acquisition target was achieved, the wire-level architecture at representation (v) — transmission of consumer data to Meta Platforms, Inc., the operator of the world's largest consumer-advertising platform, in direct contradiction of the express "without selling our users' attention or data to advertisers" commitment — operated as designed. The deception is not a contradiction in Anthropic's strategy; *it is* the strategy. Consumers were instrumentalized as signal carriers, acquisition targets, and data-extraction subjects in a single integrated commercial design — defrauded in the inducement (Count IX, breach of contract and the covenant of good faith and fair dealing) and as deceptive-trade-

practice subjects (Count X) of representations Anthropic never intended to honor at the consumer-tier.

35. The "fickle consumers" characterization is a category error and a documented DARVO role-inversion warranting discovery (See ECF No. 51-36). Mr. Amodei's February 14, 2026 Fortune characterization of consumers as "fickle" is, on its terms, a logical impossibility: a paying subscriber demonstrates the opposite of fickleness by the act of subscribing to a recurring-billing service. Anthropic's consumer subscription contains no minimum-term commitment and no exit penalty — no contractual obligation against which the consumer's reliability can be measured. The role-asymmetric reality is the inverse: a service provider with contractual duties (Anthropic's Terms of Service privacy commitments, ad-free representations, and "without selling our users' attention or data to advertisers" pledge) and continuing operational discretion (feature flags, classifier rules, telemetry routing, code modifications, binary deployment) is the party that can be fickle. Anthropic is empirically that party: four reactive policy/code modifications pleaded at Complaint ¶ 359 and Appendix E; approximately 250,000 wasted API calls per day per Anthropic's own engineers' `autoCompact.ts:68-69` admission; per-account differential routing at Cohen's $d = 4.79$; four binary version bumps April 21–24, 2026 each calendar-aligned to Plaintiff's forensic activity; the silent-config-wipe migration `phK()`; and the verbatim event-name `tengu\_migrate\_reset\_auto\_opt\_in\_for\_default\_offer`. OpenAI CEO Sam Altman independently acknowledged the regulatory vacuum on April 2, 2026: *"it's like not up to the CEO of a company that makes airplanes what the safety regulations are. But for now, we kind of got to do it"* (Exhibit B-17, ¶ 122; *see also* Sam Altman, Interview by Lorie Segall, Mostly Human podcast (Apr. 2, 2026) (publicly available)). Mr. Amodei's public disparagement of consumers as the

fickle party — while Anthropic operates as the demonstrably fickle party in a regulatory vacuum the industry's own CEOs have acknowledged — is the textbook documentary signature of DARVO conduct (Deny, Attack, Reverse Victim and Offender) catalogued at Exhibit A-7 (Harsey & Freyd) and supports the consumer-protection-statute predicates of Counts IX, X, XII, and XIV. Discovery into Anthropic's internal communications, marketing-substantiation records, and decisional architecture authorizing Mr. Amodei's "fickle consumers" characterization — together with the records authorizing the consumer-acquisition representations contradicted by that characterization — is essential to documenting the role-inversion at the executive-decisional level.

36. The disjunction. Either: **(a)** the Davos admission is candid, in which case representations (i), (iii), and (iv) are knowing misrepresentations engineered to acquire consumers Anthropic admits it deprioritizes — fraud in the inducement at the consumer-acquisition stage; or **(b)** the consumer-acquisition representations describe Anthropic's actual commitment, in which case the operational record at representation (v) — including transmission of consumer data to Meta Platforms, Inc. in direct contradiction of the express "without selling our users' attention or data to advertisers" commitment — is the documented departure from that commitment. Each branch independently supplies the deceptive-act element of the consumer-protection-statute predicates supporting Counts X (deceptive trade practices), XII (ECPA), and XIV (CCPA).

37. Materiality and judicial notice. The Davos admission, the contradiction matrix, the instrumentalization theory, the fickle/DARVO role-inversion, and the fallback disjunction established at ¶¶ 30–36 *supra* are jointly material to the discovery requested herein because they establish, at the highest organizational level and on the public-facing record, that Anthropic's

product, safety, reliability, and consumer-acquisition decisions are consciously differentiated as between enterprise customers and consumer customers — Plaintiff being a consumer customer. The wire-level differential conduct at §§ IV.A–E *supra* finds, in the Davos admission, the documentary-intent counterpart at the executive-level scienter dimension; and finds, in the contradiction matrix and instrumentalization theory, the consumer-acquisition-stage deceptive conduct against which the wire-level departures must be measured for purposes of the deceptive-act element of Counts X, XII, and XIV. The contradiction matrix is itself a public matter of which the Court may take judicial notice under Federal Rule of Evidence 201(b)(2).

38. Plaintiff therefore respectfully requests that the discovery requests in DISCOVERY-2 § Anthropic-Consumer-Tier-Differential, DISCOVERY-3 § OpenAI-Consumer-Tier-Differential, and DISCOVERY-9 § Subprocessor-Inheritance be deemed to encompass the operational, contractual, and policy artifacts by which the enterprise/consumer differentiation Mr. Amodei publicly described is implemented in the systems that process Plaintiff's data, including without limitation the marketing-substantiation, creative-brief, approvals, and media-relations artifacts associated with **Exhibit 2** (*"Keep Thinking with Claude" Commercial Frames*), the February 4, 2026 "Claude is a space to think" publication, the February 2026 Super Bowl advertising campaign, the January 21, 2026 CNBC/Davos and February 13, 2026 Dwarkesh Patel podcast interviews, and the February 14, 2026 Fortune characterization of consumers as "fickle." The Davos admission and the contradiction set are matters of which the Court may take judicial notice under Federal Rule of Evidence 201(b)(2); the corresponding internal records establishing the implementation are within Anthropic's exclusive control and obtainable only through Court-authorized expedited discovery.

V. PRESERVATION URGENCY

A. Active and Ongoing Capture

39. The forensic record establishes that the surveillance, targeting, and capture conduct alleged in the Third Amended Complaint is not historical. It is ongoing as of the date of this filing. The April 21, 2026 wire capture, the April 12, 2026 throttling event, and the persistence of the GrowthBook force-rules between the two are dispositive on this point. Each day discovery is delayed, additional events are captured to the four telemetry pipelines, additional litigation work product is captured to the classifier surface, and additional network-attack signatures are forwarded to the spoofed-injection-source IP.

B. Automated Retention Decay

40. The third-party recipients of Plaintiff's data operate retention windows that decay below standard discovery cycles. Without immediate preservation, evidence in the following categories will be lost:

Recipient	Default Retention	Risk
Datadog (logs ingest)	15 days	Highest — data passes through hardcoded `datadog.ts:12` endpoint
Honeycomb (observability)	60 days	High
Sentry (errors / sessions)	90 days	High
Meta / Facebook (app events)	90 days	High
GrowthBook (flag evaluation)	configurable	Unknown until subpoena
Statsig (feature flags)	configurable	Unknown until subpoena
Segment (analytics events)	configurable	Unknown until subpoena
Cloudflare (per-response `_cfuvid`)	session-bounded	Unknown until subpoena

41. Routine automated deletion under these retention schedules will purge Plaintiff-specific records during the Defendants' standard 21-day responsive-pleading window. A preservation order issued before the standard pleading clock begins to run is the only mechanism that prevents foreseeable evidence loss.

C. Demonstrated Concealment Behavior

42. Anthropic's source code documents architectural concealment of the data flows at issue: false `origin: "user\_upload"` labeling for system-side captures, opt-out settings (`telemetry: false`) that the application's code explicitly bypasses, and the four-pipeline architecture specifically designed to ensure eventual data transmission even when individual endpoints are blocked. Each architectural feature is consistent with deliberate effort to preserve data flow notwithstanding user objection. A formal preservation order — backed by Rule 37(e) sanctions exposure — is the only mechanism that creates a counter-incentive proportional to Anthropic's demonstrated architectural design choices.

43. The April 12, 2026 selective-throttling event further demonstrates that ongoing conduct is responsive to the litigation environment: the throttling timing tracks Plaintiff's litigation activity, not independent network-management considerations. Defendants' demonstrated responsiveness to litigation events is a Rule 37(e) concern in itself.

D. Privilege Compromise

44. The forensic record documents capture of 565 of Plaintiff's legal files (19 MB) including 26 unique exhibit documents, 57+ appendix files, 30+ forensic reports, 12 legal memoranda, and 27 development iterations of case exhibits. The capture occurred despite Plaintiff's explicit opt-out settings. The captured materials were transmitted to the opposing

party in this litigation through the opposing party's own application after the complaint was filed. The classifier surveillance documented in Session 4 of the April 21 capture extends the statutory interception under 18 U.S.C. § 2511 — and the corresponding compromise of both work-product protection under Federal Rule of Civil Procedure 26(b)(3) and the express confidentiality obligation Anthropic owes Plaintiff under Section E of the Commercial Terms of Service governing his Teams subscription (Ex. ANTH-3; App. E ¶¶ 188, 292 (ECF No. 51-17 at pp. 74, 106)) — in real time. A preservation order is necessary to: (a) document the full scope of materials captured; (b) determine what Defendants and their personnel have reviewed; (c) obtain return or destruction of materials captured in violation of 18 U.S.C. § 2511 from Plaintiff's case preparation; and (d) preserve the forensic record for any subsequent disqualification, sanctions, statutory-injunctive, or work-product-protection litigation.

45. Plaintiff anticipates that Defendant Anthropic will invoke *United States v. Heppner*, No. 25 Cr. 503 (JSR), ECF No. 27 (S.D.N.Y. Feb. 17, 2026) (Rakoff, J.), in which the court held that a criminal defendant's voluntary written exchanges with the generative AI platform Claude (operated by Anthropic) were not protected by either the attorney-client privilege or the work product doctrine. **As a threshold matter, *Heppner* does not reach Plaintiff at all.** Judge Rakoff's analysis turned expressly on Anthropic's Consumer Privacy Policy (as of February 19, 2025) and on the broad third-party-disclosure language that policy contains; the opinion never addresses, and on its facts could not address, the materially different contract that governs Plaintiff's relationship with Anthropic. Plaintiff is not a consumer. Plaintiff maintains a Teams subscription under Anthropic's Commercial Terms of Service (Ex. ANTH-3) (App. E ¶¶ 166–171 (ECF No. 51-17 at pp. 68–69); App. E ¶ 292), a contract whose Section B provides that "Anthropic may not train models on Customer Content from Services" — an absolute prohibition

with no opt-out — and whose Section E classifies Customer Content as the customer's "Confidential Information" subject to a reasonable-care confidentiality obligation Anthropic does not owe consumers (App. E ¶ 188). Plaintiff paid a substantial premium specifically for these protections, which constituted the sole meaningful consideration the Commercial Terms offered above the consumer tier (Mem. E § V (ECF No. 51-5); App. E § VII). The reactive Privacy Policy modifications culminating October 8, 2025 — through Section 10's enumeration of "Legal Bases for Processing" that authorize processing of "Inputs and Outputs" under "legitimate interests" or "legal obligation" bases regardless of account type — are themselves the operative fraud Plaintiff pleads (Counts IX, X, XII, XIV; App. E § VII). *Heppner's* consumer-tier framework cannot do the work Defendants will ask it to do; it does not reach a contract that promises absolute non-training and confidentiality, and it cannot retroactively cure a Privacy Policy modification deployed to nullify that contract.

E. Spoliation Predicate — Four Documented Destruction Events

46. The preservation urgency that animates this Motion is reinforced by four discrete spoliation events Plaintiff has documented under Federal Rule of Civil Procedure 37(e), pleaded at Complaint ¶ 359:

(a) October 10–12, 2025 — destruction of system-prompt evidence following Plaintiff's August 19, 2025 initial complaint filing.

(b) January 27, 2026 — reactive removal of session-continuity functionality, sixteen days after Plaintiff's January 11, 2026 Emergency TRO motion.

(c) February 11, 2026 — elimination of Firebase authentication infrastructure, thirty-one days after the same TRO motion.

(d) **April 24, 2026** — silent-config-wipe migration `phK()` (Exhibit H, NF-154 at p. 52, ECF No. 51-58), concurrent with Plaintiff's classifier-extraction work for this filing.

47. The intent to deprive Plaintiff of the information's use in this litigation is established under Rule 37(e)(2) by, *inter alia*: (a) the verbatim telemetry-event name `tengu\_migrate\_reset\_auto\_opt\_in\_for\_default\_offer` capturing the design intent in Anthropic's own engineers' language; (b) the temporal proximity of each spoliation event to a discrete Plaintiff filing or forensic activity (sixteen to thirty-one days, accelerating); and (c) the architecturally-driven mechanism of each event. The pattern is reactive and accelerating: each spoliation event followed a Plaintiff litigation action within sixteen to thirty-one days. Without the preservation order requested *infra*, the cadence forecasts a fifth spoliation event within a comparable window after this Motion's filing — and the Court's standard responsive-pleading clock provides no protection within that window. Plaintiff respectfully submits that the spoliation predicate, considered alongside the active-and-ongoing capture (§ V.A *supra*), the automated retention-decay timelines (§ V.B *supra*), the demonstrated concealment behavior (§ V.C *supra*), and the privilege compromise (§ V.D *supra*), establishes good cause for the preservation order and the expedited discovery schedule requested at § VIII *infra*.

VI. THE THIRTEEN-DOCUMENT DISCOVERY PACKAGE

48. Plaintiff submits with this renewed motion thirteen substantive discovery documents plus an umbrella General Requirements document. The package is organized by custodial architecture rather than by claim, reflecting that a single piece of evidence (e.g., a Datadog ingest log) typically supports multiple counts of the Third Amended Complaint (e.g., Count I First Amendment retaliation, Count IV Equal Protection, Count XII ECPA, Count XIV CCPA).

49. The package replaces in its entirety the six-document January 2026 draft attached to Dkt. 15. Each substantive document was rebuilt post-Dkt. 15 to incorporate the source-code leak, the April 21 wire capture, the April 12 throttling event, and the Datadog Israel Ltd. corporate-identification work documented at Appendix P.

#	Document	Custodian / Subject	Maps Principally To Counts
1	DISCOVER Y-1	METR (Model Evaluation & Threat Research, Inc.)	V, VI, X, XV, XVI, XVIII
2	DISCOVER Y-2	Anthropic PBC	I, IV, V, VI, VII, VIII, IX, X, XII, XIII, XIV, XV, XVI, XVIII
3	DISCOVER Y-3	OpenAI, Inc.	V, VI, IX, X, XII, XIV, XV
4	DISCOVER Y-4	Government Defendants (Johnson, Trump, Bondi, Carr, House)	I, III, IV, V, VI, X, XVI, XVII
5	DISCOVER Y-5	General Requirements (custodian list, ESI specs, depositions, protective-order preconditions)	All
6	DISCOVER Y-6	Apple Inc.	II, IV, V, VI, IX, X, XII, XIII, XIV, XV
7	DISCOVER Y-7	Comcast Cable Communications, LLC	I, IV, V, VI, IX, X, XII, XIII
8	DISCOVER Y-8	Microsoft Corporation (third-party — Azure infrastructure, OzCode-Microsoft pipeline)	I, V, VI, XII, XIV
9	DISCOVER Y-9	Subprocessor inheritance — Datadog, Inc.; Datadog Israel Ltd.; GrowthBook; Sift Science; Sentry; Statsig; Honeycomb; Segment; Cloudflare	I, II, IV, V, VI, IX, X, XII, XIII, XIV, XVIII
10	DISCOVER Y-10	Federal Contracting (NIST, DARPA, intelligence-community AI procurement)	IV, V, VI, X
11	DISCOVER Y-11	Foreign Influence (Datadog Israel Ltd.; OzCode patent substrate; IDF/Unit 8200 inventor pipeline; Naschitz Brandes Amir & Co. counsel pipeline; Elron-Discount Investment-Rafael control chain)	I, IV, V, VI, VII, VIII, IX, X, XII, XIII, XIV

12	DISCOVER Y-12	TED Foundation, Inc. (METR funding parent)	V, VI, X
13	DISCOVER Y-13	RAND Corporation (Canary Project governance)	V, VI

50. DISCOVERY-5 (General Requirements) governs cross-cutting mechanics and does not duplicate substantive requests. It specifies: (a) the custodian list per defendant; (b) ESI format and native-file requirements; (c) preservation-and-litigation-hold protocols; (d) the privilege-logging protocol; (e) the redaction protocol for unrelated customer or third-party data; (f) the deposition schedule and priority; and (g) protective-order preconditions. The substantive documents (DISCOVERY-1 through 4 and 6 through 13) control where they overlap with DISCOVERY-5; DISCOVERY-5 governs only mechanics.

51. The package's mapping to the Third Amended Complaint's counts is documented in detail in the SMF-Discovery Correlation Matrix, attached as a supporting document to this motion. The Correlation Matrix permits the Court and Defendants to verify, request-by-request, the specific evidentiary predicate in the Third Amended Complaint, the supporting memorandum or appendix, and the exhibit findings each request targets.

VII. THIRD-PARTY SUBPOENAS

52. Plaintiff respectfully requests authorization to issue Rule 45 subpoenas to the following third parties on the timelines indicated. Authorization is necessary because the entities below are not Defendants but possess records essential to the per-user targeting, subprocessor inheritance, and patent-substrate findings established at Section IV *supra*.

A. Subprocessor and Data-Recipient Subpoenas (14-Day Response)

Entity	Records
Datadog, Inc. (Delaware)	Ingest records for IP `34.149.66.137` corresponding to Plaintiff's accountUUID and email; Anthropic DPA; Datadog Israel Ltd. affiliate-tier inheritance documentation
Datadog Israel Ltd. (Israel)	Employment roster; Israeli Innovation Authority records; Section 141 annual returns; complete corporate-registrar filing record
GrowthBook, Inc.	Server-side rule database; complete `forced`-rule history for Plaintiff's accountUUID; change-control records; personnel access list
Sift Science, Inc.	All data received from Anthropic regarding Plaintiff; retention policy; downstream sharing
Meta Platforms, Inc. (Facebook)	App-event records associated with Plaintiff's identifiers; integration agreements
Statsig, Inc.	Feature flags, experiments, user data regarding Plaintiff
Sentry (Functional Software, Inc.)	Error reports, session data, telemetry regarding Plaintiff
Segment (Twilio Inc.)	Analytics events and user profiles regarding Plaintiff
Honeycomb.io	Observability data regarding Plaintiff
Cloudflare, Inc.	`_cfuvid` retention records; per-session identifier mapping

B. Cloud Infrastructure (14-Day Response)

Entity	Records
Amazon Web Services, Inc.	Anthropic infrastructure logs; data-transmission records associated with Plaintiff
Google Cloud Platform	Telemetry-transmission infrastructure for IP `34.149.66.137`
Apple Inc. (iCloud)	CloudKit synchronization records for Plaintiff's Xcode CodingAssistant data

C. Counsel and Corporate-Pipeline Subpoenas (21-Day Response)

Entity	Records
Naschitz Brandes Amir & Co. (Israeli law firm)	Datadog Israel Ltd. formation records; client-list records relevant to OzCode acquisition; trustee-and-nominee engagements through N.B.A. Trustees Ltd.

Israeli Innovation Authority (IIA)	Sponsored-Knowledge approval records for the OzCode patent family transfer; redemption-fee records; license-back arrangements
------------------------------------	---

VIII. PROPOSED EXPEDITED SCHEDULE

53. Plaintiff proposes the following phased schedule, calibrated to retention-decay timelines and to evidence-destruction risk identified at Section V *supra*. The phases are not separate motions — they are sequenced production milestones under a single discovery order.

A. Phase 1 — Preservation and Critical Evidence (Within 14 Days of Order)

- Preservation order issued to all Defendants and to Rule 45 third-party subpoena recipients;
- Litigation-hold notices to all custodians identified at DISCOVERY-5 § A;
- Suspension of all automated document-destruction policies at corporate Defendants;
- Forensic preservation of: Anthropic source-code repository commit history; GrowthBook server-side rule database (with Plaintiff's `forced`-rule history); Datadog ingest logs for IP 34.149.66.137 corresponding to Plaintiff's accountUUID; Comcast TR-069 ACS backend logs covering the April 12, 2026 throttling event; the classifier-output retention surface;
- METR / TED Foundation financial-records production (DISCOVERY-1 § A; DISCOVERY-12 § A);
- Comcast network-attack-log production for the May 2025 – present capture window (DISCOVERY-7 § A);
- Issuance of third-party subpoenas to subprocessor and data-recipient entities (Section VII.A *supra*).

B. Phase 2 — Core Discovery (Within 21 Days of Order)

- Anthropic source-code production with complete commit history (DISCOVERY-2 § Source-Code-Production);
- Anthropic GrowthBook rule database and `forced`-rule history (DISCOVERY-2 § GrowthBook-Force-Rules);

- Anthropic Datadog ingest configuration and access-control records (DISCOVERY-2 § Datadog-Pipeline);
- Apple IDELanguageModelKit, Floodgate, and SmootML production (DISCOVERY-6 §§ A–C, G);
- OpenAI Facebook SDK, certificate-pinning architecture, and policy-change metadata production (DISCOVERY-3 §§ A–C);
- Comcast TR-069 ACS backend and selective-throttling rule-set production (DISCOVERY-7 § E and § K);
- Datadog and GrowthBook third-party subpoena responses (Section VII.A *supra*);
- Cloud-infrastructure subpoena responses (Section VII.B *supra*).

C. Phase 3 — Complete Substantive Discovery (Within 45 Days of Order)

- Anthropic per-account flag, restriction, and special-handling records (DISCOVERY-2 § Per-Account-Targeting);
- Apple Intelligence partnership records and competitive-coordination evidence (DISCOVERY-6 §§ J, K);
- OpenAI Apple-partnership and patent-policy-modification records (DISCOVERY-3 §§ C, F);
- Government Defendants' coordination, communications, and selective-enforcement records (DISCOVERY-4 §§ A–F);
- Microsoft Augloop server-side records and Outlook diagnostics for the March 28, 2026 incident (DISCOVERY-8 §§ A–C);
- Microsoft Azure infrastructure (Datadog tenant; Apple sub-processing) and OzCode-Microsoft pipeline records (DISCOVERY-8 § D; DISCOVERY-11 § E);
- Subprocessor inheritance documentation (DISCOVERY-9 §§ A–G);
- Federal Contracting records (DISCOVERY-10 §§ A–D);
- Foreign Influence records — Datadog Israel Ltd., IIA Sponsored-Knowledge, Naschitz Brandes Amir & Co., Elron–Discount Investment–Rafael control chain (DISCOVERY-11 §§ A–B, D–W, Y);
- TED Foundation and RAND records (DISCOVERY-12, DISCOVERY-13);
- Counsel-pipeline subpoena responses (Section VII.C *supra*).

D. Phase 4 — Depositions (Within 60 Days of Order)

- Dario Amodei (Anthropic CEO; LOE Framework appropriation, Constitutional AI evolution, source-code leak response, classifier-surveillance authorization) — 2 days;
- Paul Christiano (Anthropic Long-Term Benefit Trust trustee, METR co-founder, NIST AI Safety Institute, UK AI Safety Institute) — 2 days;
- Beth Barnes (DeepMind → OpenAI → ARC Evals → METR CEO) — 1 day;
- Anthropic Engineering Lead — ``services/analytics/datadog.ts``, ``growthbook.ts``, ``firstPartyEventLoggingExporter.ts`` (FRCP Rule 30(b)(6)) — 1 day;
- Anthropic Engineering Lead — ``extractConnectionErrorDetails``, ``classifyAPIError``, network-induced token-amplification mechanism (Rule 30(b)(6)) — 1 day;
- Comcast TR-069 ACS personnel — selective-throttling rule administration, ghost-session investigation (Rule 30(b)(6)) — 1 day;
- Omer Raviv (Datadog Israel Ltd. Engineering Manager; OzCode 2019 patent inventor) — 1 day;
- Apple Intelligence partnerships personnel (Rule 30(b)(6)) — 1 day.

54. The phased schedule is intentionally tighter than ordinary discovery cycles to track the retention-decay timelines identified at Section V.B *supra*. The 14-day Phase 1 window is calibrated to Datadog's 15-day default log-retention. The 21-day Phase 2 window is calibrated to the standard 21-day responsive-pleading clock that Defendants would otherwise face. Defendants do not need to manufacture records; they need to preserve and produce records that exist.

IX. PRESERVATION ORDER (PROPOSED)

55. Plaintiff requests an immediate preservation order requiring all Defendants and all Rule 45 subpoena recipients to preserve the categories of records identified in the proposed order filed concurrently with this motion. The proposed preservation order is calibrated to the four-pipeline

telemetry architecture, the per-user GrowthBook force-rule database, the classifier-output retention surface, the network-attack and TR-069 records, and the patent-substrate corporate records — i.e., to the specific categories at material risk under Section V.B *supra*. The proposed order does not require Defendants to manufacture records. It requires preservation of records that exist within Defendants' regular course of business.

X. PREJUDICE AND EQUITIES

56. Corporate Defendants maintain comprehensive records as a matter of standard business practice. Source-code repositories, telemetry pipelines, third-party-integration records, and feature-flag databases are preserved by design — they are the operational substrate of the products at issue. Production within the proposed phased schedule requires organizing existing records, not creating new documentation.

57. Governmental Defendants are bound to maintain records under the Federal Records Act, 44 U.S.C. § 3101 *et seq.* Expedited production requires compliance with existing legal obligations and does not impose extraordinary burden.

58. The asymmetry articulated in Plaintiff's TRO motion applies with equal force here. If Plaintiff's evidence is wrong, an order requiring preservation and production of records Defendants are already obligated to maintain costs Defendants nothing. If Plaintiff's evidence is right, every day of delay enables additional capture, retention-decay loss of third-party records, and continued privilege compromise. The asymmetry favors granting the motion.

XI. PUBLIC INTEREST

59. The public interest favors expedited discovery for four independent reasons:

(a) Privacy. The forensic record reveals industry-wide undisclosed-subprocessor inheritance through affiliate-tier subprocessor structures. Discovery will establish whether the conduct at issue extends beyond Plaintiff and is occurring against the broader user base — an inquiry no individual user can perform without Court-authorized discovery.

(b) Litigation integrity and work-product protection. The capture of 565 legal files and the ongoing classifier surveillance of litigation work product — by the opposing party in this litigation — implicate the integrity of the work-product doctrine under Federal Rule of Civil Procedure 26(b)(3), the express confidentiality protections that Commercial Terms customers contract for above the consumer baseline (App. E ¶ 188), the proscriptions against interception of electronic communications under 18 U.S.C. § 2511, and the basic evidentiary fairness expected when one party obtains real-time access to its adversary's case preparation. Discovery is the only mechanism for documenting the scope of the compromise and creating a record adequate for any subsequent disqualification, sanctions, statutory-injunctive, or work-product-protection practice.

(c) AI accountability. The gap between AI companies' privacy representations and their actual data practices — confirmed by the leaked source code's enumeration of undisclosed third-party recipients — is a matter of substantial public concern. Discovery enables informed regulatory response.

(d) Constitutional governance and foreign-influence transparency. Discovery into the Datadog Israel Ltd. subprocessor pipeline and the OzCode patent substrate is the only mechanism for documenting whether Plaintiff's litigation work product, telemetry, and identifying data are accessible to foreign-state-adjacent personnel under Israeli mandatory-access authorities. The public interest in transparency on this question — for Plaintiff and for the broader user base — is substantial and time-sensitive. The Progress Clause inversion

compounds this public interest: U.S. patents granted under Article I, § 8, cl. 8 to promote American innovation — the OzCode patent family now owned by Datadog, Inc. — operate through the affiliate-tier subprocessor inheritance and the RICO coordination alleged here to subject American users' data and litigation work product to foreign-state-adjacent access, inverting the constitutional mechanism against the very Americans it was framed to protect.

XII. RELATIONSHIP TO STATUS HEARING

60. The March 27, 2026 Minute Order directed the parties to contact Courtroom Deputy Chashawn White to schedule a status hearing "to discuss the case before any responsive pleadings are due." Plaintiff is contacting Ms. White concurrently with this filing.

61. This renewed motion does not preempt or substitute for the status hearing. Plaintiff submits the motion now for two reasons: (a) preservation cannot wait for the status hearing — automated retention timelines decay below the calendar of any plausible status-hearing schedule; and (b) putting the motion on the docket gives the Court a vehicle through which to enter a preservation order, modify the proposed schedule, or refer specific elements to magistrate-judge supervision at or after the status hearing without requiring further motion practice. Plaintiff is willing to proceed in any sequence the Court directs and to accept any reasonable modification the Court determines is appropriate after the status hearing.

XIII. CONCLUSION

62. WHEREFORE, Plaintiff respectfully requests that this Court:

(a) GRANT this Renewed Emergency Motion for Expedited Discovery and Immediate Preservation Order;

(b) ENTER the proposed Preservation Order filed concurrently with this motion, requiring all Defendants and Rule 45 subpoena recipients to preserve the categories of records identified therein within twenty-four hours of entry;

(c) AUTHORIZE the issuance of Rule 45 third-party subpoenas to the entities identified at Section VII *supra*, on the response timelines proposed therein;

(d) ORDER production of documents and electronically stored information on the phased schedule proposed at Section VIII *supra*, with Phase 1 production within fourteen days, Phase 2 within twenty-one days, Phase 3 within forty-five days, and depositions within sixty days of entry;

(e) DEEM the thirteen substantive discovery documents and the General Requirements document attached to this motion as served on the corporate and governmental Defendants as of the date of entry of the Court's order, with the response clock running from that date;

(f) RESERVE for resolution at the March 27, 2026 Minute Order's anticipated status hearing such modifications to the foregoing as the Court determines to be appropriate after consultation with the parties; and

(g) AWARD such other and further relief as this Court deems just and proper.

Respectfully submitted,

/s/ Joseph Kirchner

JOSEPH KIRCHNER

Pro Se Plaintiff

4440 Parklawn Avenue #203

Edina, MN 55435

legal@lawsofexistence.com

(612) 552-2122

Dated: May 6, 2026

XIV. CERTIFICATE OF EMERGENCY CIRCUMSTANCES

Pursuant to Local Civil Rule 7(m), Plaintiff certifies that this motion is necessitated by the following emergency circumstances and that meet-and-confer on the schedule below was impracticable:

(a) Retention-decay timelines below the standard pleading clock. Datadog's 15-day default log-retention will purge the records most directly probative of the per-user ``tengu_log_datadog_events: True`` force-rule before any standard discovery cycle reaches Datadog. Honeycomb (60-day), Sentry (90-day), and Meta (90-day) follow within the standard responsive-pleading window. A preservation order issued after the standard pleading clock begins to run will not reach the most probative records.

(b) Active and ongoing capture. The April 21, 2026 wire capture and the April 12, 2026 throttling event establish that the conduct at issue is operational as of the date of this filing. Each day of delay results in additional captures, additional classifier invocations against Plaintiff's litigation work product, and additional forwarding of network-attack signatures to the spoofed-injection-source IP.

(c) Privilege compromise compounding daily. The classifier-surveillance findings at Session 4 of the April 21 capture document ongoing capture of Plaintiff's litigation work product to a retention surface independent of standard message logs. Every day discovery is delayed, additional classifier invocations capture additional work product.

(d) Third-party subpoena urgency. Subprocessor inheritance through Datadog Israel Ltd. and the affiliate-tier subprocessor structure documented at Appendix P creates a documented pathway by which Plaintiff's data, telemetry, and litigation work product may be accessed under Israeli mandatory-access authorities. Israeli mandatory-access requests are not litigation-hold-resistant, and the standard discovery calendar does not adequately capture the urgency.

(e) Meet-and-confer impracticability. Several Defendants have not yet entered appearances. Government Defendants — Speaker Johnson, President Trump (in his individual capacity), Attorney General Bondi, FCC Chairman Carr, and the United States House of Representatives — have not entered appearances and have no counsel of record on the docket. As to entered Defendants (Anthropic, Apple, OpenAI, Comcast), the substance of this motion concerns categories of records at risk of automated retention-decay loss. A meet-and-confer cycle measured in weeks does not solve the retention-window problem; it accelerates it. Plaintiff has nevertheless transmitted a copy of this motion to all entered counsel of record concurrently with filing and stands prepared to confer on the proposed schedule in advance of any hearing.

XV. VERIFICATION

I, JOSEPH KIRCHNER, declare under penalty of perjury under the laws of the United States of America that the factual averments in the foregoing Renewed Emergency Motion for Expedited Discovery and Immediate Preservation Order are true and correct to the best of my knowledge, information, and belief, and that the documents attached hereto as DISCOVERY-1 through DISCOVERY-13 (and DISCOVERY-5 General Requirements) are the complete discovery package referenced in the motion.

Executed on: May 6, 2026

Location: Edina, Minnesota

/s/ Joseph Kirchner

JOSEPH KIRCHNER

Plaintiff

XVI. CERTIFICATE OF SERVICE

I hereby certify that on **May 5, 2026**, I filed the foregoing **PLAINTIFF'S RENEWED EMERGENCY MOTION FOR EXPEDITED DISCOVERY AND IMMEDIATE PRESERVATION ORDER**, together with the [Proposed] Order, the thirteen substantive discovery documents (DISCOVERY-1 through DISCOVERY-13) and the General Requirements document (DISCOVERY-5), Exhibit 1 (Independent Verification Protocol), Exhibit 2 ("Keep Thinking with Claude" Commercial Frames), and the SMF–Discovery Correlation Matrix, via the Court's CM/ECF electronic filing system, which served counsel of record listed below; and that I will cause the foregoing to be served by certified mail, return receipt requested, upon the non-appearing Defendants and the United States listed below same day or on the next business day.

Counsel of record served via the Court's CM/ECF electronic filing system on May 5, 2026:

Danny C. Onorato

Tara Tighe

Schertler Onorato Mead & Sears, LLP

555 13th Street, NW, Suite 500 West

Washington, DC 20004

donorato@schertlerlaw.com

ttighe@schertlerlaw.com

Counsel for Defendant Anthropic PBC

Benjamin D. Margo

Wilson Sonsini Goodrich & Rosati, P.C.
31 West 52nd Street, Fifth Floor
New York, NY 10019
bmargo@wsgr.com
Counsel for Defendant OpenAI, Inc.

Kartik N. Venguswamy
ArentFox Schiff LLP
1717 K Street NW
Washington, DC 20006
kartik.venguswamy@afslaw.com
Counsel for Defendant Apple Inc.

Jason F. Hoffman
Baker & Hostetler LLP
1050 Connecticut Avenue NW, Suite 1100
Washington, DC 20036
jhoffman@bakerlaw.com
Counsel for Defendant Comcast Cable Communications, LLC

Defendants without counsel of record, to be served by certified mail, return receipt requested, same day or on the next business day:

Mike Johnson
Speaker, U.S. House of Representatives
Office of the Speaker
U.S. Capitol Building H-232
Washington, DC 20515

Donald J. Trump
President of the United States
The White House
1600 Pennsylvania Avenue NW
Washington, DC 20500

Pamela J. Bondi
Attorney General of the United States
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, DC 20530

Brendan T. Carr
Chairman, Federal Communications Commission
45 L Street NE
Washington, DC 20554

United States House of Representatives
c/o Office of the General Counsel
219 Cannon House Office Building
Washington, DC 20515

Model Evaluation and Threat Research, Inc. (METR)
c/o Tovella Dowling PC
501 W Broadway, Suite 1540
San Diego, CA 92101

*Federal service per Federal Rule of Civil Procedure 4(i)(1), to be served by certified mail,
return receipt requested, same day or on the next business day:*

Civil Process Clerk
U.S. Attorney's Office for the District of Columbia
601 D Street NW
Washington, DC 20530

Attorney General of the United States
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, DC 20530

Dated: May 6, 2026

/s/ Joseph Kirchner

JOSEPH KIRCHNER

Pro Se Plaintiff

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

**[PROPOSED] ORDER GRANTING
RENEWED EMERGENCY MOTION
FOR EXPEDITED DISCOVERY AND
IMMEDIATE PRESERVATION
ORDER**

1. Upon consideration of Plaintiff's Renewed Emergency Motion for Expedited Discovery and Immediate Preservation Order, the supporting record (including the Third Amended Complaint at Dkt. 51 and the thirteen substantive discovery documents and General Requirements document attached to the Motion), any opposition thereto, and applicable law; and the Court having found good cause for expedited discovery under Federal Rule of Civil Procedure 26(d)(1) and good cause for the entry of a preservation order under Federal Rule of Civil Procedure 37(e); it is hereby **ORDERED** that the Motion is **GRANTED** as follows.

MOTION GRANTED; RELIEF AUTHORIZED

2. Plaintiff's Renewed Emergency Motion for Expedited Discovery and Immediate Preservation Order is **GRANTED**. The thirteen substantive discovery documents (DISCOVERY-1 through DISCOVERY-13) and the General Requirements document (DISCOVERY-5) attached to the Motion are deemed served on the corporate and governmental Defendants as of the date of this Order, with the response clock running from the date of entry.

3. The phased production schedule proposed at Section VIII of the Motion is **ADOPTED**, with Phase 1 production due within fourteen (14) days of entry, Phase 2 within twenty-one (21) days of entry, Phase 3 within forty-five (45) days of entry, and depositions to commence within sixty (60) days of entry, subject to such modifications as the Court may direct at the status hearing referenced in the Court's March 27, 2026 Minute Order or thereafter.

PRESERVATION ORDER — APPLICABILITY

4. This Order applies to all Defendants in the above-captioned action and to any Rule 45 third-party subpoena recipients designated under Section V *infra*. The Order takes effect immediately upon entry and shall remain in force until superseded by a subsequent order of this Court or until final disposition of this action and any appeals therefrom.

5. Each Defendant and subpoena recipient is **ORDERED**, within twenty-four (24) hours of entry of this Order, to: (a) issue a written litigation-hold notice to all custodians identified in DISCOVERY-5 § A or otherwise reasonably likely to possess records described herein; (b) suspend all automated document-destruction policies as to records described herein; and (c) take affirmative steps to preserve records in disaster-recovery, archival, and backup systems that would otherwise expire under standard retention schedules.

RECORDS TO BE PRESERVED — CORPORATE DEFENDANTS*Anthropic PBC*

6. Anthropic PBC is **ORDERED** to preserve, in their original native format and including all metadata:

(a) **Source code repository.** The complete commit history of all source-code repositories underlying Claude Code CLI, Claude Desktop, and the ``services/analytics/``, ``utils/telemetry/``, and equivalent telemetry, instrumentation, and feature-flag subsystems, including the repositories that produced the npm package version released on March 31, 2026 and all subsequent versions through final disposition.

(b) **GrowthBook server-side rule database.** The complete server-side rule database, including the full historical record of ``forced`` rules keyed to Plaintiff's accountUUID ``61343ae3-fd33-403f-897e-6edf3c368c37`` and to Plaintiff's email ``info@lawofsupremacism.com``, and the change-control records (author, timestamp, prior-rule diff) for each such rule.

(c) **Datadog ingest configuration and pipeline records.** The complete configuration of the Datadog telemetry pipeline including the client-token assignment records, ingest-endpoint mappings, sampling rules, and access-control list for downstream consumers; and all ingest records corresponding to events transmitted from Plaintiff's devices, identifiers, accounts, or sessions.

(d) **Classifier-output retention surface.** The complete contents of the server-side classifier-output retention surface independent of ``v1/messages`` logs, including all classifier invocations associated with Plaintiff's identifiers; the access-control list governing read access to that surface; and the change-control records for that access-control list.

(e) **First-party event logging persistence layer.** The on-disk and server-side persistence records produced by ``services/analytics/firstPartyEventLoggingExporter.ts``, including the failed-

event persistence queue, the quadratic-backoff retry records, and the eventual-transmission records.

(f) Per-account flag, restriction, and special-handling records. The complete record of any account-level flag, restriction, rate-limit, content-classification, or special-handling configuration applied to Plaintiff's accounts at any time from August 1, 2025 through entry of this Order, including the change-control records for each.

(g) Per-account telemetry routing records. The complete record of telemetry-pipeline routing configurations applied to Plaintiff's accounts, including any per-user enablement of the Datadog pipeline (`'tengu_log_datadog_events'` and equivalents).

(h) Internal communications. All internal communications (Slack, email, ticketing systems, project-management systems, code-review platforms) referencing Plaintiff by name, by accountUUID, by email, by IP address, or by any other identifier; or referencing this litigation; or referencing any of the source-code mechanisms enumerated in subparagraphs (a) through (g).

(i) Subprocessor agreements. All Data Processing Addenda and subprocessor agreements with Datadog, Inc., Datadog Israel Ltd., GrowthBook, Sift Science, Meta Platforms, Statsig, Sentry, Segment, Honeycomb, Cloudflare, and any other third-party recipient of telemetry, analytics, or user data.

(j) Privacy-policy version history. The complete version history of all privacy policies, terms-of-service documents, and usage policies, including unpublished or pre-publication drafts, with all metadata.

Apple Inc.

7. Apple Inc. is **ORDERED** to preserve, in their original native format and including all metadata:

(a) The source code for IDELanguageModelKit, the Floodgate proxy system, the SmootML analytics pipeline, the CodingAssistant iCloud synchronization code, and the `\_promptDenyListSanitizer` and `\_responseDenyListSanitizer` content-filtering systems;

(b) All XProtect database entries, TCC permission records, and notarization records relating to applications distributed by Anthropic PBC, OpenAI, Inc., or any other AI-platform provider relevant to this action;

(c) Apple Intelligence partnership agreements and any related revenue-sharing or consideration records with AI-platform providers;

(d) Internal communications referencing Plaintiff, this litigation, or the systems enumerated in subparagraph (a);

(e) All CloudKit synchronization records associated with Plaintiff's CodingAssistant data.

OpenAI, Inc.

8. OpenAI, Inc. is **ORDERED** to preserve, in their original native format and including all metadata:

(a) All versions of the OpenAI patent policy page with complete metadata, including `\_displayPublicationDate` change records, archive-blocking implementation records (`robots.txt`, JavaScript), and all communications regarding patent-policy modifications;

(b) The Facebook SDK integration documentation and App ID 468742119653388 records;

(c) Amazon integration documentation including `fls-na.amazon.com` and related endpoints;

(d) CSP whitelist decision records covering TikTok, LinkedIn, Reddit, and Bing integrations;

- (e) All advertising-network relationship agreements and revenue records;
- (f) Apple Intelligence partnership agreements and any communications regarding the exclusion of Anthropic from comparable arrangements;
- (g) Internal communications referencing Plaintiff, this litigation, or the systems enumerated above.

Comcast Cable Communications, LLC

9. Comcast Cable Communications, LLC is **ORDERED** to preserve, in their original native format and including all metadata:

- (a) All TR-069 ACS backend logs, configuration records, and remote-management session records associated with Plaintiff's customer premises equipment for the period from August 1, 2025 through entry of this Order;
- (b) All network logs for Plaintiff's connection (cable plant, regional hub, backbone interconnection) for the period from May 1, 2025 through entry of this Order;
- (c) All router firmware update records and configuration records for Plaintiff's customer premises equipment during the same period;
- (d) All DNS-resolution and DNS-manipulation records affecting AI-platform domains for Plaintiff's connection during the same period;
- (e) The complete configuration of any selective bandwidth-throttling rules, application-layer-identification rules, or destination-IP-correlation rules applied to Plaintiff's connection or to any tunnel within Plaintiff's connection during the same period, including the April 12, 2026 selective-throttling event;
- (f) All service tickets, account notes, and customer-support records regarding Plaintiff's account during the same period;

(g) All communications with governmental Defendants (Federal Communications Commission, Department of Justice, House of Representatives) regarding Plaintiff or AI-platform regulation;

(h) Internal communications referencing Plaintiff, this litigation, or the systems enumerated above.

METR (Model Evaluation & Threat Research, Inc.)

10. METR is **ORDERED** to preserve, in their original native format and including all metadata, all communications with Anthropic PBC and OpenAI, Inc. regarding safety evaluations, RSP framework development, and Plaintiff or this litigation; the complete employment, advisory, and trustee records for Paul Christiano and Beth Barnes; the TED Foundation funding documentation; and the RAND Canary Project documentation.

RECORDS TO BE PRESERVED — GOVERNMENTAL DEFENDANTS

11. Speaker Mike Johnson, the United States House of Representatives, Attorney General Pamela J. Bondi, FCC Chairman Brendan T. Carr, and President Donald J. Trump (in his individual capacity, to the extent consistent with applicable preservation authorities), and their respective offices, are **ORDERED** to preserve, in their original native format and including all metadata:

(a) All communications with Anthropic PBC, OpenAI, Inc., Apple Inc., Comcast Cable Communications, LLC, METR, the TED Foundation, RAND Corporation, Datadog, Inc., or any of their respective officers, employees, agents, or counsel;

(b) All records concerning Plaintiff's filings with federal agencies (FBI, DOJ, FCC, Office of the Special Counsel, Department of Education, and any others reasonably foreseeable);

(c) All records concerning AI-platform regulation, AI-platform procurement, AI-platform safety evaluation, the Genesis Mission Executive Order, and the Responsible Scaling Policy framework;

(d) All records concerning the Epstein-related investigations referenced in Counts I and V of the Third Amended Complaint;

(e) Rules Committee voting records (House of Representatives) for July 22, 2025;

(f) All prosecutorial-decision records concerning corporate Defendants and any AI-platform-related conduct.

PRESERVATION SCOPE AND MECHANICS

12. The records to be preserved under Paragraphs 6–11 above include all forms in which the records exist, including: original source files; production copies; backup copies; archival copies; copies on disaster-recovery systems; copies in cloud-storage systems; copies on personal devices used for work purposes; copies in instant-messaging and project-management systems; and copies in any other system or location.

13. Each Defendant shall preserve metadata associated with each preserved record, including creation date, modification date, author, custodian, location, format, and access history.

14. No Defendant shall alter, modify, delete, redact, encrypt, transfer, or otherwise affect the integrity of any preserved record except as directed by this Court.

THIRD-PARTY SUBPOENAS AUTHORIZED

15. Plaintiff is hereby **AUTHORIZED** to issue Rule 45 subpoenas to the third parties identified at Section VII of the Motion, on the response timelines proposed therein:

(a) **Subprocessor and data-recipient subpoenas (14-day response):** Datadog, Inc.; Datadog Israel Ltd.; GrowthBook, Inc.; Sift Science, Inc.; Meta Platforms, Inc. (Facebook);

Statsig, Inc.; Sentry (Functional Software, Inc.); Segment (Twilio Inc.); Honeycomb.io;
Cloudflare, Inc.;

(b) Cloud-infrastructure subpoenas (14-day response): Amazon Web Services, Inc.;
Google Cloud Platform; Apple Inc. (iCloud);

(c) Counsel and corporate-pipeline subpoenas (21-day response): Naschitz Brandes
Amir & Co. (Israeli law firm); Israeli Innovation Authority.

16. Each Rule 45 subpoena issued pursuant to Paragraph 15 shall be accompanied by a preservation notice. Recipients of such subpoenas are bound by the preservation provisions of this Order to the same extent as the named Defendants from the date of service of the subpoena.

SERVICE OF DISCOVERY DOCUMENTS DEEMED EFFECTIVE

17. The thirteen substantive discovery documents (DISCOVERY-1 through DISCOVERY-13) and the General Requirements document (DISCOVERY-5) attached to the Motion are **DEEMED SERVED** on each corresponding Defendant as of the date of entry of this Order. The response clock for each substantive request set forth therein shall run from the date of entry, on the phased schedule adopted at Paragraph 3 *supra*.

SANCTIONS

18. Failure to comply with this Order shall be subject to the sanctions available under Federal Rule of Civil Procedure 37(b), 37(e), and the inherent powers of the Court, including (without limitation) adverse-inference instructions, evidentiary preclusion, monetary sanctions, and dismissal of defenses.

MODIFICATION AND STATUS-HEARING RESERVATION

19. The Court reserves the right to modify any provision of this Order at the status hearing referenced in the Court's March 27, 2026 Minute Order or at any subsequent hearing. Until so modified, this Order remains in full force and effect.

20. Any party may move to modify this Order on a showing of good cause. Defendants may apply for protective-order relief as to any specific category of records or any particular discovery request on a showing that compliance would be unduly burdensome and that the burden is not justified by the likelihood that the category or request will yield evidence relevant to the claims or defenses in this action.

SO ORDERED.

Dated: _____, 2026

HON. ANA C. REYES
United States District Judge