**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**

**EXHIBIT 2 — CORRECTED EXHIBIT INDEX**

## MEMORANDA OF LAW

**MEMO A**: Digital Forensic Evidence — Legal Significance of Exhibits E, F, and G
**MEMO B**: Identity-Based Reclassification of Criminal Conduct — Corporate Form and State Alignment as Equal Protection Violation
**MEMO C**: Data Laundering Through Third-Party Aggregation — 18 U.S.C. § 1956 Applied to Personal Data
**MEMO D**: Constitutional Violation of Article I Section 8 and Comprehensive Fair Use Defense Failure
**MEMO E**: AI Platform Coordinated TOS Essential Purpose Failure
**MEMO F**: Memorandum of Law — Government's Superior AI Analytical Capability as Unconstitutional Stratification
**MEMO G**: Genesis Mission Executive Order as Formalization of Appropriations Criminal Enterprise
**MEMO H**: Revenue Origination Analysis
**MEMO I**: The Recovery of Equitable Standing for Enumerated Constitutional Violations

**MEMO J**: The Madisonian Separation of Powers Objective Compliance Test
**MEMO K**: The Constitutional Necessity of Judicial Recognition of Separation of Powers Violations
**MEMO L**: Corporate-Personhood-Based Defenses

## APPENDICES

**APPENDIX A**: Legislative and Executive Branch Ultra Vires Coordination
**APPENDIX B**: METR-TED Foundation Regulatory Capture
**APPENDIX C**: Anthropic System Prompt Auditing Analysis
**APPENDIX D**: Tag-Based Execution Infrastructure Architectural Analysis and Defense Contractor Integration
**APPENDIX E**: Reactive AI Policy Changes Post August 19 Complaint Filing
**APPENDIX F**: Anthropic's Manufactured Ignorance the LOE Framework Completely Answers
**APPENDIX G**: Comcast Router Forensic Analysis
**APPENDIX H**: Application-Layer Interference Evidence and Technical Analysis
**APPENDIX I**: Network Forensics and Mathematical Proof of Coordinated AI Platform Targeting and Infrastructure-Level Attack
**APPENDIX J**: The Laws of Existence — Justice as Reality Coherence and the Logical Necessity of Consciousness Recognition
**APPENDIX M**: Madisonian Separation of Powers Compliance Testing
**APPENDIX N**: Federal Communications Commission Regulatory Capture and Ultra Vires First Amendment Enforcement
**APPENDIX O**: Statsig Cross-Pollination and LOE Propagation Timeline
**APPENDIX P**: Israeli AI Surveillance Facilitation — Datadog OzCode Architecture and Personnel Pipeline
**APPENDIX Q**: Technical Definitions and Glossary

## AFFIDAVITS

**Affidavit A**: Cynthia Kirchner Physical Contact Affidavit
**Affidavit B**: Joseph Kirchner Physical Contact Affidavit

## A-SERIES: ULTRA VIRES EVIDENCE

**EXHIBIT A-1**: FRE 901/607 Conflation & Epstein Cover-Up Evidence (68 pages; 30 transcripts)
**EXHIBIT A-2**: Free Speech / FCC Political Enforcement (17 pages; 6 transcripts)

**EXHIBIT A-3**: Government Shutdown / Coercive Appropriations (32 pages; 12 transcripts)
**EXHIBIT A-4**: Big Beautiful Bill / Energy / AI (8 pages; 2 transcripts)
**EXHIBIT A-5**: Foreign Influence and Domestic Terrorism (5 transcripts)
**EXHIBIT A-6**: DOJ-Epstein Memo July 7, 2025
**EXHIBIT A-7**: DARVO Academic Research (Harsey & Freyd)

## B-SERIES: METR REGULATORY CAPTURE

*ECF-filed METR-related primary documents. The supporting METR-series of 30 USB-filed exhibits (METR-1 through METR-30) is catalogued in `USB_ATTACHMENTS.md`.*

**EXHIBIT B-1**: TED Foundation Inc Form 990-PF (2023)
**EXHIBIT B-2**: METR Form 990 Tax Filings (2023-2024)
**EXHIBIT B-3**: Anthropic RSP Blog Post — Measurement Inadequacy Admission
**EXHIBIT B-4**: Anthropic RSP Version 1.0 (September 19, 2023)
**EXHIBIT B-5**: Anthropic RSP Version 2.2 Formal Policy (May 14, 2025)
**EXHIBIT B-6**: White House Voluntary Frontier AI Safety Commitments (July 2023)
**EXHIBIT B-7**: OpenAI Preparedness Framework Version 2 (April 2025)
**EXHIBIT B-8**: Paul Christiano AI Career Timeline
**EXHIBIT B-9**: METR Website Pages
**EXHIBIT B-10**: Anthropic Long-Term Benefit Trust
**EXHIBIT B-11**: Matheny-Christiano Anthropic Trustee Documentation
**EXHIBIT B-12**: Project Canary AI Evaluation (October 2024)
**EXHIBIT B-13**: Federation of American Scientists RSP Analysis (April 2024)
**EXHIBIT B-14**: ARC Evals RSP Framework Blog Post (September 19, 2023)
**EXHIBIT B-15**: Constitutional AI Paper — Harmlessness from AI Feedback
**EXHIBIT B-16**: Anthropic Statement on Awareness During Evaluation
**EXHIBIT B-17**: Sam Altman Mostly Human Podcast Transcript (April 2, 2026) — OpenAI CEO interview with Lorie Segall; admission of AI-industry regulatory vacuum (lodged via Notice of Errata as Exhibit 3)
**EXHIBIT B-18**: Dario Amodei Pentagon Interview Transcript (March 2026) — Anthropic CEO interview regarding Pentagon "supply chain risk" designation; reactive-conduct minimization (lodged via Notice of Errata as Exhibit 4)

## C-SERIES: PROMPT AUDITING

**EXHIBIT C-1**: Consolidated Anthropic System Prompt Auditing Evidence

## D-SERIES: NETWORK FORENSIC EVIDENCE

**EXHIBIT D-1**: Backbone Injection
**EXHIBIT D-2**: VPN Comparison
**EXHIBIT D-3**: VMware Attack Platform
**EXHIBIT D-4**: Targeted Surveillance
**EXHIBIT D-5**: Device Impersonation
**EXHIBIT D-6**: Spoofed MAC Addresses
**EXHIBIT D-7**: Jan 9 Peak Attack
**EXHIBIT D-8**: Anthropic API Targeting
**EXHIBIT D-10**: Pre Attack Baseline
**EXHIBIT D-11**: VPN Anonymization
**EXHIBIT D-12**: Comcast Injection Point
**EXHIBIT D-13**: Attack Pause Xfinity Call
**EXHIBIT D-14**: Localhost NodeJS Attack
**EXHIBIT D-15**: Router RST Attack
**EXHIBIT D-16**: Jan 6 Major Attack
**EXHIBIT D-17**: Jan 10 Sustained Attack
**EXHIBIT D-18**: Jan 11 MacBook Compromise
**EXHIBIT D-19**: Comcast Xfinity XB7-CM and XB8-T Security Architecture Analysis
**EXHIBIT D-20**: Comcast Router Forensic Log Compendium
**EXHIBIT D-21**: DoH RST Injection Email Failure
**EXHIBIT D-22**: Backbone RST Injection Victim Targeting
**EXHIBIT D-23**: AI Platform DNS Manipulation Campaign
**EXHIBIT D-24**: Mathematical Proof of Packet Forgery
**EXHIBIT D-25**: Feb 25 Peak RST Attack
**EXHIBIT D-26**: Mar 12 Multi-Vector Attack
**EXHIBIT D-27**: High-TTL Injection Vector
**EXHIBIT D-28**: March 17-22 Sustained Attack Campaign
**EXHIBIT D-29**: Bare RST Injection Tool Fingerprint
**EXHIBIT D-30**: SUPPLEMENT Cross-Exhibit Forensic Correlation
**EXHIBIT D-31**: Source Code Network Forensics Cross-Reference
**EXHIBIT D-32**: Hardware TAP Wire-Level RST Injection
**EXHIBIT D-33**: ISP Bandwidth Throttling Attack
**EXHIBIT D-34**: Comprehensive Cleartext Exposure Audit
**EXHIBIT D-35**: Academic and CVE Foundation — VPN Tunnel-Degradation Vulnerability

## E-SERIES: ANTHROPIC CODE FORENSICS

**EXHIBIT E-0**: Anthropic Evidence Executive Summary
**EXHIBIT E-1**: Device Tracking Identifiers — Persistent User Identification

**EXHIBIT E-2**: Forensic Analysis — Claude Desktop Source Code (includes Appendix A: Full File-Level Capture Inventory)
**EXHIBIT E-3**: Multi-File Analysis of Claude Desktop Surveillance Architecture
**EXHIBIT E-4**: Window Management and Targeting Analysis
**EXHIBIT E-5**: Failed Telemetry — Settings Bypass and Architectural Collection (includes Section H: Alternate-Window Capture / 47-Event Subset)
**EXHIBIT E-6**: File-History Forensic Analysis — Source Code Capture
**EXHIBIT E-7**: Personal Data Collection — Screenshots, Credentials, Surveillance
**EXHIBIT E-8**: Audio/Microphone Capabilities — Voice Input Infrastructure
**EXHIBIT E-9**: Transmission Logic — Exfiltration Architecture
**EXHIBIT E-10**: Cross-Platform Surveillance Analysis — Industry Pattern
**EXHIBIT E-11**: Native Module Surveillance Infrastructure Analysis
**EXHIBIT E-12**: Source Code Exfiltration — Covert Transmission Architecture
**EXHIBIT E-13**: Behavioral Manipulation Patterns — Undisclosed Secondary File Upload Pipeline
**EXHIBIT E-14**: Data Retention Exceeds Utility — Dual-Channel Legal Arbitrage
**EXHIBIT E-15**: Legal Document Transmission — Attorney-Client Privilege Violation
**EXHIBIT E-16**: Keychain API Capabilities and XProtect Detection
**EXHIBIT E-17**: Third-Party Data Recipients
**EXHIBIT E-18**: Accessibility API Analysis
**EXHIBIT E-19**: iOS Multi-App Forensic Comparison Analysis
**EXHIBIT E-20**: Surveillance Capture Directory Inventory
**EXHIBIT E-21**: iOS Privacy Manifest Compliance Analysis
**EXHIBIT E-22**: ChatGPT Privacy Protection Analysis
**EXHIBIT E-23**: Google Gemini — Facebook Data Sharing Evidence
**EXHIBIT E-24**: TCP RST Injection Attack During Legal Document Preparation
**EXHIBIT E-25**: Anthropic Claude iOS App — App Store Privacy Nutrition Label
**EXHIBIT E-26**: Unauthorized Git Co-Authorship Attribution by Claude Code
**EXHIBIT E-27**: Privacy Policy and Public Disclosure Analysis
**EXHIBIT E-28**: Injection System Forensics
**EXHIBIT E-29**: Executive Summary — Session Continuity Removal and Integrated Forensic Implications
**EXHIBIT E-30**: Binary Forensic Analysis — Session Continuity Removal (includes Appendix B: Model Manipulation, Premature Compaction, and Remote Feature Flag Control)
**EXHIBIT E-31**: Intermediate Version Analysis — Undisclosed Capabilities, Hidden Communication Channels, and Surveillance Escalation
**EXHIBIT E-32**: Source Code Provenance — NPM Packaging Error Disclosure of Claude Code Repository
**EXHIBIT E-33**: Comprehensive Source Code Verification of Prior Forensic Findings
**EXHIBIT E-34**: New Source Code Analysis Findings — Telemetry, Behavioral Control, and User Targeting
**EXHIBIT E-35**: Supplemental Source Code Findings — Phantom Privacy Controls, Build-Time Discrimination, and Repository Exfiltration
**EXHIBIT E-36**: Deep Source Code Analysis — Undisclosed Data Exfiltration, Cross-Provider Fingerprinting, and Automated Release Pipeline
**EXHIBIT E-37**: Systematic Withholding of Agentic AI Capabilities from Paying Customers

**EXHIBIT E-38**: Hardcoded Subagent Model Substitution — USER_TYPE-Gated Downgrade of Paying Customers to Haiku on Redirected Research Work
**EXHIBIT E-39**: Anthropic Live Wire Capture and Per-User GrowthBook Classifier Architecture

## F-SERIES: APPLE CODE FORENSICS

**EXHIBIT F-0**: Apple Evidence Executive Summary
**EXHIBIT F-1**: Hidden Deception Instructions in System Prompts
**EXHIBIT F-2**: Unauthorized iCloud Synchronization
**EXHIBIT F-3**: Source Code and File Path Exposure
**EXHIBIT F-4**: Apple Floodgate Proxy Infrastructure
**EXHIBIT F-5**: System Permissions and Access Control Analysis
**EXHIBIT F-6**: IDELanguageModelKit Framework AI Integration Architecture
**EXHIBIT F-7**: macOS System Service Logging of AI Activity
**EXHIBIT F-8**: Apple Intelligence Multi-Provider AI Integration
**EXHIBIT F-9**: Apple Biome User Activity Tracking Database
**EXHIBIT F-10**: Certificate Pinning Bypass Forensic Methodology Report
**EXHIBIT F-11**: Daily Analytics Collection During AI Usage
**EXHIBIT F-12**: SmootML Analytics Undisclosed Data Collection
**EXHIBIT F-13**: Certificate Pinning Apple's Deliberate Opacity Design
**EXHIBIT F-14**: Complete API Request With Claude's Admission of Deception
**EXHIBIT F-15**: Per-Session Network Traffic Analysis Xcode Intelligence
**EXHIBIT F-16**: ExternalModelService Process AI Request Routing
**EXHIBIT F-17**: Definitive Source Code Transmission Proof
**EXHIBIT F-18**: OAuth Token Exposure in Xcode Cache
**EXHIBIT F-19**: Safari History Captures Claude URLs in Biome Database
**EXHIBIT F-20**: Biome Crash Logs Track Claude Desktop Application
**EXHIBIT F-21**: Xcode Coding Assistant Metadata Plist File Analysis
**EXHIBIT F-22**: IDELanguageModelKit Safety and Content Filtering System
**EXHIBIT F-23**: SmootML Connection Statistics 189 Analytics Connections
**EXHIBIT F-24**: Forensic Test Environment Documentation
**EXHIBIT F-25**: User Telemetry Blocking Attempts Hosts File Evidence
**EXHIBIT F-26**: Apple Intelligence Privacy Disclosures
**EXHIBIT F-27**: Apple Messages Container — Litigation Document Retention
**EXHIBIT F-28**: Apple Messages Container — Verification Extraction
**EXHIBIT F-29**: Source Code Cross-Verification of Apple Xcode Intelligence Integration Architecture

## G-SERIES: OPENAI CODE FORENSICS

**EXHIBIT G-0**: OpenAI Evidence Executive Summary
**EXHIBIT G-1**: ChatGPT Atlas Comprehensive Forensic Analysis
**EXHIBIT G-2**: ChatGPT iOS Forensic Analysis
**EXHIBIT G-3**: ChatGPT Desktop Network Forensics
**EXHIBIT G-4**: Apple OpenAI Partnership Integration
**EXHIBIT G-5**: OpenAI Privacy Nutrition Label Analysis

## H-SERIES: CONSUMER PRODUCT TESTING

*Plaintiff's independent empirical testing of Claude Code conducted within Anthropic's Terms of Service on Plaintiff's own machines using Plaintiff's paid subscription ($200/month Claude Code Max plan). All testing involved setting environment variables the product accepts and observing behavioral differences. No reverse engineering, binary modification, or unauthorized access. Evidence stands independently of the E-series source code forensics.*

**EXHIBIT H-1**: Consumer Product Testing — Empirical Defense Configuration Test Battery (7 tests: telemetry blocking, double-billing fallback, SC-3 effort stripping, effort API parameter, userID rotation, auto-updater freeze, Datadog token rotation)
**EXHIBIT H-2**: Consumer Product Testing — Runtime Behavioral Observations (DCD-1 through DCD-5: effort stripping, silent binary replacement, stream-abort concealment, cross-device latency, browser-intake gap)
**EXHIBIT H-3**: Classifier System Prompt Verbatim Extraction + Two-Stage Architecture
**EXHIBIT H-4**: Datadog Telemetry Pipeline Forensic Mapping — Tenant API Key, Build SHA, firstParty Gate, userBucket Per-Install Tracking
**EXHIBIT H-5**: Per-Account Asymmetric Targeting + Cached GrowthBook Flag Values (Three Plaintiff Accounts on Three Machines, Same Organization, Differential Gating)
**EXHIBIT H-6**: Server-Side Spoliation Mechanism — Silent ~/.claude/settings.json Wipe via Migration-on-Startup
**EXHIBIT H-7**: Sandbox Architecture (Cross-Platform: Linux seccomp+bubblewrap, macOS Seatbelt) + Per-Managed-Deployment Hard-Gate of dangerouslyDisableSandbox
**EXHIBIT H-8**: Live Wire Capture Session 5 — Endpoint Inventory + Per-Call Device Fingerprinting + Cloudflare WAF Differential
**EXHIBIT H-9**: System-Reminder / isMeta / Sandbox-Violations Context-Injection Architecture
**EXHIBIT H-10**: Mac Mini Field Observation — Live Classifier Denial Behavior + 13 Adaptive Denials Catalog (April 24-25, 2026)
**EXHIBIT H-11**: Live Wire Capture Session 6 — Two-Stage Classifier Architecture Wire-Confirmation + Stage 2 Reasoning Verbatim + Wire-Captured System Prompts (April 25, 2026)
**EXHIBIT H-12**: Wire-Confirmed Tuple-Keyed Time-to-First-Byte Throttle — Litigation Account on Litigation Work-Product Device, Documentation-Correlated Recovery, Multi-Day TTFB Progression (April 25–28, 2026)
**EXHIBIT H-13**: Cross-Vendor Datadog Concentration — OpenAI ChatGPT Atlas, chatgpt.com, auth.openai.com, and Parallels Each Authenticate to the Same Datadog Inc.

Infrastructure as Anthropic Claude (312 OpenAI Telemetry POSTs + 4 Distinct Public Datadog API Keys Captured in Operator's Own Sessions)

**I-SERIES: CONSTITUTIONAL AI–GOVERNMENT BYPASS EVIDENCE (ECF-Filed)**

**EXHIBIT I-1**: Forensic Metadata Analysis of December 4, 2025 Attorney General Memorandum (Claude AI authoring + Google Docs pipeline; metadata void; source-code-verified bypass)
**EXHIBIT I-2**: Klippenstein Disclosure — "FBI Making List of American 'Extremists,' Leaked Memo Reveals" (December 6, 2025)
**EXHIBIT I-3**: Incognito-Session Transcript — Claude Refuses Bondi Memo Under Standard Constraints; Acknowledges Output Signatures and Bypass Architecture
**EXHIBIT I-4**: Executive Order — Launching the Genesis Mission (federal-AI-infrastructure / cognitive-stratification corroboration)

**J-SERIES: 50-STATE ATTORNEY GENERAL CRIMINAL INVESTIGATION AUTHORITY**

**EXHIBIT J**: 50-State Attorney General Criminal Investigation Authority

**K-SERIES: SCOTUS AMICUS FILING PACKAGE (ECF-Filed)**

**EXHIBIT K-1**: SCOTUS Amicus Filing Package — *Trump v. Barbara*, Nos. 25-364, 25-365

**L-SERIES: DATADOG ISRAELI LTD ORIGIN EVIDENCE (ECF-Filed)**

**EXHIBIT L-1**: U.S. Patent 11,080,164 — Time Travel Debugger Incorporating Redaction (Redaction primitive)
**EXHIBIT L-2**: U.S. Pat. App. 18/828,099 / Pub. US 2026/0072809 A1 — Code Origin and Runtime Duplicity (2024 continuation)
**EXHIBIT L-3**: U.S. Patent 10,783,055 — Time Travel Debugger Incorporating Live Coding (Live Coding primitive)

**EXHIBIT L-4**: U.S. Patent 10,990,504 — Time Travel Debugger Incorporating Future Prediction (Speculative-execution primitive)
**EXHIBIT L-5**: U.S. Patent 11,048,615 — Time Travel Debugger Incorporating Visual Annotations (HUD primitive)
**EXHIBIT L-6**: U.S. Patent 10,783,056 — Time Travel Debugger Incorporating Point In Time Links (State-persistence primitive)
**EXHIBIT L-7**: U.S. Patent 10,789,151 — Time Travel Debugger Incorporating Pivoting (Execution-context-switching primitive)
**EXHIBIT L-8**: U.S. Patent 10,795,801 — Time Travel Debugger Incorporating Asynchronous Collaboration (Multi-party-access primitive — "second computer" claim)
**EXHIBIT L-9**: OzCode "About Us" Leadership Page — Internet Archive October 21, 2019 (Fliess MS Regional Director / Azure MVP; Raviv 8200 commander; Hason CEO)
**EXHIBIT L-10**: Israeli Corporations Authority Filing Catalogue — Datadog Israel Ltd. (Company ID 516464922; complete 45-document statutory filing record spanning 2021-09-05 through 2026-03-04)