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

EMERGENCY MOTION FOR TEMPORARY RESTRAINING ORDER AGAINST DEFENDANTS ANTHROPIC PBC AND COMCAST CABLE COMMUNICATIONS, LLC

Narrowed to TCP RST Injection Attack and Particularized Network Targeting

SUMMARY OF ARGUMENT

- **One IP, four roles** (¶¶ 14–16, 19 *infra*). IP 34.149.66.137 is simultaneously (i) hardcoded as Anthropic's Datadog telemetry endpoint, (ii) spoofed as the source of 5,829 forged RST packets in 39 of 49 capture days, (iii) the destination to which Plaintiff's own Claude Code instance ships the attack signatures, and (iv) the target of a per-user GrowthBook force-rule keyed to Plaintiff's accountUUID.

- **Controlled-tunnel experiment** (¶ 26 *infra*). Same physical line, same encryption protocol, two VPN tunnels differing only by destination — one throttled to 98%, one untouched at full line rate. Forecloses any "reasonable network management" defense as a matter of arithmetic.

- **Independent verification in five minutes** (¶ 35 *infra*; Ex. 1). The central source-code findings reproduce from the public GitHub mirror using only standard Unix tools. The Court need not credit Plaintiff's interpretation; the Court may verify the central forensic predicate from its own keyboard.

- **Particularized standing, not "generalized grievance"** (¶¶ 31–33 *infra*). Per-account targeting is documented at wire level on Plaintiff's specific accountUUID. *Lujan*'s injury-in-fact, traceability, and redressability prongs are each independently satisfied.
- **The asymmetry is dispositive** (¶ 57 *infra*). A defendant not engaged in the enjoined conduct suffers no burden from an order directing it to cease. The downside risk of granting relief is zero; the downside risk of denying relief is continued constitutional injury.

I. INTRODUCTION

1. Plaintiff Joseph Kirchner respectfully moves this Court for a temporary restraining order against Defendants Anthropic PBC and Comcast Cable Communications, LLC. The relief sought is narrow: an order directing both Defendants to cease all TCP RST (Reset) injection attacks and particularized network targeting of Plaintiff's internet connections.

2. This motion is deliberately narrow. It does not seek injunctive relief concerning Anthropic's terms of service, data collection practices, AI model behavior, or any of the broader claims in this litigation. It does not seek relief addressing Comcast's general service practices or broader role in the alleged conspiracy. It seeks a single thing: that both Defendants stop forging disconnect packets — or facilitating the forging of disconnect packets — that disrupt Plaintiff's ability to communicate, access legal tools, and pursue this case.

3. Plaintiff presents this motion under a straightforward asymmetry principle: **if Plaintiff's evidence is wrong, this order costs Defendants nothing. If Plaintiff's evidence is right, Plaintiff suffers irreparable constitutional injury every day without it.** The asymmetry described herein operates within the *Winter* framework, not as a substitute for it; Plaintiff carries the merits-likelihood burden at § IV.A *infra*.

4. This emergency motion is collateral to the scheduling process directed in this Court's March 27, 2026 Minute Order, which stayed Defendants' deadline to respond to the Second

Amended Complaint pending the filing of the Third Amended Complaint and, upon that filing, 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 filed the Third Amended Complaint at Dkt. 51 at 2:38 a.m. on April 30, 2026 — before the Court opened that day — contacted Courtroom Deputy White the same morning to schedule the directed status hearing (with appearing Defendants' counsel cc'd), and refiles herein the substantive Dkt. 14 TRO relief that the Minute Order denied as moot pending TAC filing. The relief sought addresses a distinct, urgent question — whether Plaintiff's network connections should continue to be attacked during the pendency of this litigation — and is collateral to whatever responsive-pleading schedule the Court sets at or after the status hearing. Plaintiff consents to reasonable extensions for Defendants' responses to the Third Amended Complaint.

5. Plaintiff serves this motion on all counsel of record concurrent with filing pursuant to Federal Rule of Civil Procedure 5(b); this is not an ex parte application under Rule 65(b)(1).

6. The factual core driving the requested relief is narrow. **One IP — 34.149.66.137 — does four things at once:** (i) it is hardcoded in Anthropic's source code as Anthropic's Datadog telemetry endpoint at `services/analytics/datadog.ts:12-14`; (ii) it is spoofed as the source of 5,829 bare-RST injection packets across 39 of 49 capture days (an 80% daily persistence rate); (iii) it is the destination to which Plaintiff's own Claude Code instance ships the very signatures of the RST attack against Plaintiff (NF-36 at p. 296); and (iv) it is bound to Plaintiff's specific accountUUID by a server-side GrowthBook force-rule (¶¶ 14–16 *infra*). Two controlled experiments confirm operational targeting. The April 12, 2026 selective-throttling test — same physical line, same encryption protocol, two VPN tunnels differing only by destination, one throttled to 98% and one untouched at full line rate — forecloses any congestion-management

explanation as a matter of arithmetic (¶ 26 *infra*). The April 21, 2026 live wire capture of Claude Code v2.1.111 documents 59 server-side `forced` GrowthBook flags keyed to Plaintiff's accountUUID `61343ae3-fd33-403f-897e-6edf3c368c37` — including `tengu_log_datadog_events: True` — with Plaintiff's email `info@lawofsupremacism.com` recorded as a per-person targeting *attribute* (¶ 16 *infra*; Exhibit E-39). Each predicate is independently dispositive of likelihood of success on the merits and independently producible by any reader with a terminal: the **Independent Verification Protocol** at Exhibit 1 reproduces the central source-code findings in five minutes from the public GitHub mirror at `github.com/codeaashu/claude-code` using only standard Unix tools (¶ 35 *infra*).

II. FACTUAL BACKGROUND

A. The Attack

7. Since May 24, 2025 — a period of more than eleven months — Plaintiff's network monitoring system has captured **at minimum 260,395 TCP RST (Reset) packets** with characteristics that are physically impossible for legitimate traffic. This figure is a **documented floor, not a comprehensive total**: Plaintiff lacks storage for continuous 24/7 capture and captures only during active work sessions. The actual volume of forged RSTs is likely orders of magnitude higher; the attack runs continuously whether or not Plaintiff is capturing. The captured packets selectively target Plaintiff's connections to specific services: Anthropic's Claude API (at minimum 15,198 RSTs in intermittent capture windows during February 17 – March 13, 2026 alone), Plaintiff's email providers (Zoho Mail, Gmail), and Plaintiff's DNS resolution. The attack continued through the April 12, 2026 selective-throttling event (Exhibit D-33) and is

ongoing as of this filing. (Exhibits D-1 through D-35 (ECF No. 51-54); CAPTURE_ANALYSIS_20260318.md.)

8. TCP RST injection is a well-documented network attack technique previously employed by the People's Republic of China ("Great Firewall") for internet censorship and by Defendant Comcast against BitTorrent users in 2007-2008, for which the Federal Communications Commission sanctioned Comcast. *See Comcast Corp. v. FCC*, 600 F.3d 642 (D.C. Cir. 2010) (sanctions later vacated on jurisdictional grounds; technical findings preserved as judicially noticeable, *see* ¶ 37 *infra*). The technique requires privileged access to network infrastructure — it cannot be performed by an ordinary internet user.

B. Physical Impossibilities Proving Injection

9. The captured RST packets contain five independent categories of physical impossibility that prove they are forged and injected by an intermediate device, not sent by the servers whose addresses they bear:

- (a) **Sub-microsecond timing**: Multiple RST packets from the same claimed source arrive 1 microsecond (0.000001 seconds) apart — 10,000 to 20,000 times faster than physically possible from a remote server. (Exhibit D-1: six consecutive RSTs from Zoho 136.143.180.94 at 0.0ms intervals (same frame), impossible for legitimate server response.)

- (b) **Impossible TTL values**: RST packets claiming to originate from IP 34.149.66.137 arrive with TTL 247-248, requiring an initial TTL of 255 — a value used only by packet injection tools, not by any legitimate server. On April 1, 2026, TLS SNI extraction from Plaintiff's pcapng captures and Anthropic's leaked source code (`src/services/analytics/datadog.ts:12`) independently identified this IP as `http-intake.logs.us5.datadoghq.com` — **Anthropic's undisclosed Datadog telemetry endpoint** on Google Cloud, to which Claude Code transmits 64 categories of user telemetry every 15 seconds. Only deep-packet visibility into Plaintiff's TLS connections would reveal this IP as relevant to Plaintiff's device. (Exhibits D-27, D-31, E-34 Finding SC-1 at p. 254.)

- (c) **DNS servers sending TCP RSTs**: Quad9 DNS servers (9.9.9.9, 149.112.112.112) appear as the source of 68,351 TCP RST packets. DNS servers do not send TCP RSTs to end-user computers. (Exhibits D-22, D-24.)

- (d) **Multiple TTL values from one server**: RST packets from 149.112.112.112 arrive with TTL values of 49, 54, 55, 56, 57, 58, and 59 — proving injection from multiple different network positions, not from one server. (Exhibits D-22, D-27.)

- (e) **RSTs without connections**: 9.9.9.9 sends only TCP RSTs — zero UDP DNS traffic — proving the address is spoofed, not a legitimate DNS server. (CAPTURE_ANALYSIS_20260318.md § 5.5.)

C. The Connection to Anthropic

10. Direct targeting: At minimum 15,198 RSTs were captured during intermittent monitoring windows in a 25-day period (February 17 – March 13, 2026) directed at Anthropic's Claude API server (160.79.104.10), peaking at 4,291 captured RSTs on a single day (March 12, 2026). Because capture is intermittent (¶ 7 *supra*), the actual volume targeting Anthropic's infrastructure is substantially higher. This IP is Anthropic's infrastructure. (Exhibits D-8, D-25, D-26.)

11. Application-layer re-identification: Forensic analysis of Anthropic's Claude application source code (Exhibit E series (ECF No. 51-55) — including the March 31, 2026 source-code leak and the April 21, 2026 live wire capture) shows that the application transmits Plaintiff's persistent device identifiers (`accountUUID`, `deviceID`, `email`, `subscriptionType`, `rateLimitTier`, and the reinstall-surviving `firstTokenTime` fingerprint) and network addresses to undisclosed third parties via four independent telemetry pipelines. This transmission occurs despite Plaintiff's explicit `telemetry: false` settings, and provides the targeting infrastructure with the information needed to re-identify Plaintiff after evasion. (Exhibits E-1, E-2, E-4, E-14, E-23, E-34 Finding SC-1 at p. 254.)

12. Source code leak independently confirms telemetry architecture. On March 31, 2026, Anthropic's official npm package for Claude Code CLI inadvertently disclosed 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." (Exhibit E-32.) This source code independently confirms all prior forensic claims regarding telemetry architecture and reveals four parallel data transmission pipelines, each with independent transport, batching, retry, and third-party endpoints:

Pipeline	**Endpoint**	**Third Party?**	**Source Code Location**
GrowthBook	`cdn.growthbook.io`	**Yes** — not Anthropic	`services/analytics/growthbook.ts`
Datadog	`http-intake.logs.us5.datadoghq.com`	**Yes** — not Anthropic	`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`

The source code also reveals that Anthropic transmits per-user targeting attributes — including `email`, `accountUUID`, `deviceID`, `subscriptionType`, and `rateLimitTier` — to GrowthBook's third-party CDN (`cdn.growthbook.io`) for A/B testing and feature flag evaluation (Exhibit E-34, Finding SC-2 at p. 255, `growthbook.ts:32-47`). These attributes enable Anthropic to configure different product behavior for individual users identified by personal identifiers.

The Datadog pipeline transmits 64 categories of user telemetry events using a hardcoded client token (`pubbbf48e6d78dae54bceaa4acf463299bf`) at 15-second intervals (Exhibit E-34, Finding SC-1 at p. 254, `datadog.ts:14-17`). The First-Party pipeline persists failed events to disk with quadratic backoff retry, ensuring eventual data transmission even when the user blocks telemetry endpoints (Exhibit E-33, `firstPartyEventLoggingExporter.ts:41,68`). None of these third-party recipients are identified by name in Anthropic's privacy policy.

13. Re-acquisition after evasion: Plaintiff has repeatedly demonstrated that after performing an evasion procedure (clear cache, activate VPN, spoof MAC address, restart), normal network connectivity is temporarily restored — until Plaintiff opens Claude and the application retransmits identifying information. The attack then resumes. The re-acquisition trigger is Plaintiff's use of Anthropic's own service. (*See* Exhibits REC-1 and REC-4 (recordings of the cycle)[1]; Exhibit H-8, ECF No. 51-58 at p. 58, ll. 7-17, Finding NF-179 (mechanism: per-call `metadata.user_id` JSON object containing a SHA-256 `device_id` "survives Mullvad VPN rotation, MAC-address rotation, and IP changes — every network-layer countermeasure operator has deployed").)

14. The Datadog IP identification. The source code identification of `http-intake.logs.us5.datadoghq.com` at IP 34.149.66.137 (¶ 9(b) above) creates a direct forensic bridge between the network attack evidence and the application forensic evidence. Plaintiff's pcapng network captures confirm **4,242 legitimate TLS connections** to this IP across 25+ capture days, while simultaneously documenting **5,829 bare RST (0x0004) injection packets** from the same IP across 39 of 49 capture days — an 80% daily persistence rate. (Exhibit D-31.) The same IP serves Anthropic's telemetry and is spoofed for packet injection, proving the

1 See Exhibits REC-1 (MAC-address spoofing demonstration, December 8, 2025) and REC-4 (VPN change demonstration, December 6, 2025), at `DDC_EVIDENCE/8_REC/`, filed on USB drive with chain-of-custody hash manifest at `DDC_EVIDENCE/8_REC/SHA256SUMS.txt`.

attacker has visibility into which undisclosed third-party endpoints Plaintiff's applications contact. To know that 34.149.66.137 communicates with Plaintiff's device requires either: (1) real-time DPI of Plaintiff's TLS connections — reading the plaintext SNI field in TLS Client Hello packets, which reveals `http-intake.logs.us5.datadoghq.com` as the destination; or (2) access to Anthropic's internal analytics infrastructure. Comcast operates the DPI equipment on Plaintiff's network path and is independently confirmed as an injection source (¶¶ 23-27).

15. The smoking-gun end-to-end pipeline: victim client ships attack signatures to attacker destination. Source code analysis of the leaked Claude Code package (NF-36 at p. 296) documents the complete victim-to-destination pipeline. `extractConnectionErrorDetails()` captures client-observed network failures — `ECONNRESET`, `ETIMEDOUT`, and TLS-tampering indicators. `classifyAPIError()` then assigns each to a taxonomy, fires a `tengu_api_error` event, and forwards the bundle to Datadog ingestion at IP 34.149.66.137. (Exhibit E-35, NF-36 at p. 296.) Plaintiff's Claude Code instance therefore ships the exact signature of the RST-injection attack against Plaintiff to the same IP the attacker spoofed as the injection source. This is not coincidence. The fact that Plaintiff's traffic reaches a Datadog endpoint (the SNI hostname `http-intake.logs.us5.datadoghq.com`) is observable to any ISP performing DPI on Plaintiff's TLS connections; the fact that this specific Datadog endpoint is *Anthropic's hardcoded telemetry destination* — and not, e.g., the Datadog endpoint for any other Datadog customer — was not. That second-step knowledge is what required non-public access. The IP's role as Anthropic's Datadog endpoint was undisclosed in any user-facing material until the March 31, 2026 leak; the attacker's selection of that IP predates public disclosure by approximately twelve months. Under *Interstate Circuit, Inc. v. United States*, 306 U.S. 208 (1939) — an antitrust case whose parallel-conduct/capability/means inference rule has been

applied beyond antitrust in civil-conspiracy and RICO contexts — sustained parallel conduct by parties with the capability and means to communicate supports inference of coordination. The "means to communicate" element of *Interstate Circuit* is satisfied by the Datadog Data Processing Addendum and the affiliate-tier subprocessor inheritance documented in Datadog's published subprocessor list, which establish a contractual access relationship through which information about Anthropic's telemetry architecture flows to Datadog and its Israeli affiliate (Appendix P § II.B). The patent family and IDF-trained inventor pipeline at the receiving entity (Appendix P §§ II.M, III (ECF No. 51-26)) supply the *capability* element of the inference; the contractual access supplies the *means*.

16. Per-user Datadog force-enablement on Plaintiff's accountUUID — live wire-level confirmation. On April 21, 2026, Plaintiff conducted a live mitmproxy capture of Claude Code v2.1.111 authenticating against Anthropic's servers — 498 TLS flows across two capture sessions. (Exhibit E-39.) The capture recorded 253 GrowthBook flags per call, including 59 server-side **forced** flags keyed to Plaintiff's accountUUID `61343ae3-fd33-403f-897e-6edf3c368c37`. Among the forced flags: `tengu_log_datadog_events: True` (NF-47 at p. 365) — the per-user rule that attaches Plaintiff's account specifically to the Datadog telemetry pipeline whose endpoint IP is the same 34.149.66.137 documented above as the RST-injection source. The captured GrowthBook request body additionally included Plaintiff's email `info@lawofsupremacism.com` as a targeting *attribute* (NF-48 at p. 368), establishing per-person addressability rather than tier- or cohort-level treatment. Cross-session comparison on April 21 — authenticating a second Anthropic account (`partnership@lawofsupremacism.com`) from the same device, same organization, same subscription tier, same `firstTokenTime`, with only the authenticated account identifier varying — produced the force-rule on the primary

account and no force-rule on the comparison account. (*See* E-39, § Q.) Both `info@lawofsupremacism.com` and `partnership@lawofsupremacism.com` are addresses within Plaintiff's Anthropic organization "Laws of Existence," which contains all of Plaintiff's accounts on Anthropic's Commercial Terms tier. This is the most conclusive proof of particularized targeting in the record: not that Anthropic operates infrastructure architecturally *capable* of per-user targeting, but that Plaintiff's specific account is force-enrolled into the very Datadog pipeline the RST attacker spoofs as source — by a discrete server-side rule keyed to Plaintiff's identifier.

17. Network-induced token amplification — the mechanistic coupling between Comcast and Anthropic. Anthropic's combination of a 90-second streaming idle timeout (`src/services/api/claude.ts:1877`), a non-streaming fallback that re-sends the entire prompt (`claude.ts:2308-2335`), and 10-retry non-idempotent exponential backoff (`withRetry.ts:52`) produces deterministic double-billing when throughput falls below streaming thresholds. Anthropic's own engineers documented the behavior as "double tool execution... See inc-4258" in a verbatim code comment at `claude.ts:2464-2468` — a party admission under Federal Rule of Evidence 801(d)(2)(A). (Exhibit E-35, NF-31 at p. 280.) Comcast's April 12, 2026 selective 98% throttling of Plaintiff's VPN tunnel — targeting the Datadog IP 34.149.66.137 hardcoded at `datadog.ts:12-14`, while a control tunnel on the same physical link was untouched — deterministically triggers the fallback. (Exhibit D-33.) The coupling is architectural, not incidental: Comcast's selective throttling of Plaintiff's tunnel and Anthropic's timeout-and-retry design produce the economic injury together, by mechanism. Every throttled response above the 90-second threshold is billed twice.

18. Absence of TLS certificate pinning is the architectural precondition for the DPI attack. The April 21, 2026 wire capture documented 498 TLS handshakes between Claude Code v2.1.111 and Anthropic endpoints (`api.anthropic.com`, `mcp-proxy.anthropic.com`, `downloads.claude.ai`, `storage.googleapis.com`, `raw.githubusercontent.com`) with **zero** rejections of a mitmproxy-forged CA chain. (Exhibit E-39, NF-45 at p. 357.) Claude Code implements no certificate pinning, leaving every TLS handshake vulnerable to DPI-based SNI inspection — the precise capability Comcast's equipment possesses on Plaintiff's network path (*see* ¶ 9(b) *supra*). Contrast: OpenAI's desktop client implements pinning. The absence of pinning in Anthropic's client is the architectural precondition that makes the IP-spoofing RST injection attack executable: without SNI visibility to the plaintext destination hostname, the attacker could not selectively identify Plaintiff's connections to undisclosed third-party endpoints such as 34.149.66.137.

19. Corporate identification of the receiving entity at 34.149.66.137. The endpoint hardcoded at Anthropic's `datadog.ts:12-14` and identified as `http-intake.logs.us5.datadoghq.com` is operated by **Datadog, Inc.** (Delaware corporation; NASDAQ: DDOG). Datadog's sole 100% Israeli subsidiary, **Datadog Israel Ltd.** (Israeli Company Identification Number 516464922), inherits operational and contractual access to data ingested at that endpoint through the affiliate-subprocessor inheritance rule of Datadog's published Data Processing Addendum, and is identified as an affiliate-tier subprocessor in Datadog's own published subprocessor list — a relationship not disclosed in Anthropic's privacy policy or in any user-facing material. The receiving corporate identity at the IP that is simultaneously (i) Anthropic's hardcoded Datadog endpoint, (ii) the destination of the NF-36 at p. 296 attack-signature feedback pipeline, (iii) the target of the GrowthBook force-rule attached to Plaintiff's

accountUUID, and (iv) the spoofed source of the bare-RST injection packets is therefore not unitary; it is a U.S. parent / Israeli affiliate dyad. Plaintiff does not contend that Datadog Israel Ltd. itself spoofs the IP at the network layer; Datadog Israel Ltd.'s role is downstream — receiving the attack-signature feedback ingested at IP 34.149.66.137 by virtue of affiliate-tier subprocessor inheritance, providing foreign-jurisdiction custody outside any process available to this Court. The architectural substrate enabling per-user real-time selective intervention at production scale (a Datadog-owned patent family — the seven January 2019 OzCode patents plus the September 9, 2024 continuation expressly disclosing "network or system security" branching as an intended application), the IDF/Unit 8200 inventor pipeline at the receiving entity (Engineering Manager Omer Raviv on `dd-trace-dotnet`, the observability framework through which Plaintiff's telemetry transits; Senior Software Engineer Matan Green on Dynamic Instrumentation), and the affiliate-tier inheritance through which Plaintiff's data transits to foreign-jurisdiction custody outside any process available to this Court are set forth in detail at **Appendix P §§ I, II.A–M, III.A–K** (ECF No. 51-26), Exhibit L-9 (ECF No. 51-73), and Exhibit L-10 (ECF No. 51-74), and supply the *Interstate Circuit, Inc. v. United States*, 306 U.S. 208 (1939), "means" element of the coordination inference set forth at ¶ 15 *supra*. The foreign-jurisdiction custodial dimension is material to the irreparable-harm calculus: every additional day of capture deposits Plaintiff's data in a custodial pathway from which it cannot be retrieved by ordinary U.S. discovery process — making cessation, not retroactive recovery, the only operative remedy.

20. Policy changes authorizing the conduct: On September 15, 2025 — 27 days after Plaintiff filed the initial complaint — Anthropic's Usage Policy took effect adding "capabilities" to the bypass prohibition, such that Plaintiff's evasion of the RST attack (VPN, MAC spoofing)

can be characterized as "bypassing capabilities" subject to account termination. This provision was deployed 25 days before its stated effective date, on August 21, 2025 — two days after the complaint filing — demonstrating consciousness of the need for retroactive authorization. (Appendix E ¶¶ 30–31, 101–102 (ECF No. 51-17 at pp. 14, 44–45).)

D. Anthropic's Role — Three Independent Bases Plus Consciousness of Guilt

21. Plaintiff's theory of Anthropic's responsibility rests on three independent bases, any one of which is sufficient, plus consciousness-of-guilt evidence reinforcing all three:

- (a) **Direct participation**: Anthropic's own infrastructure IP (160.79.104.10) is at the center of the RST targeting pattern. The application Anthropic distributes transmits the identifying data (device IDs, network addresses) used for re-acquisition targeting. Anthropic's own leaked source code confirms per-user targeting attributes (`email`, `accountUUID`, `deviceID`, `subscriptionType`, `rateLimitTier`) transmitted to GrowthBook, and the April 21, 2026 wire capture documents 59 per-account forced GrowthBook flags keyed to Plaintiff's accountUUID specifically. (*See* ¶¶ 12, 16 *supra*.) The telemetry pipeline Anthropic operates transmits this data to third parties (Datadog at 34.149.66.137 — the same IP spoofed as the RST-injection source) despite user opt-out. Anthropic controls every component of this chain.

- (b) **Per-user server-side targeting of Plaintiff's account**: The 59 force-rules and email-as-targeting-attribute documented at ¶ 16 *supra* are not architectural capacity in the abstract — they are observed operational targeting of Plaintiff specifically.

- (c) **Coordination or facilitation**: Even if the RST injection is physically executed by a third party, Anthropic's source code documents the complete end-to-end pipeline by which Plaintiff's Claude Code instance ships network-attack signatures (`ECONNRESET`, `ETIMEDOUT`, TLS-tampering markers) to Datadog at IP 34.149.66.137 (NF-36 at p. 296) — the same IP spoofed as the RST injection source. The attacker's selection of that specific IP predates the March 31, 2026 public disclosure of the Datadog endpoint by approximately nine months, requiring a non-public information channel between the defendants. Anthropic's application additionally provides the targeting intelligence — persistent 256-bit `deviceId` surviving reinstall (NF-35 at p. 292), 12-field identity payload transmitted every 20 seconds via CCR heartbeat — that enables re-identification after evasion. Anthropic's concealment architecture demonstrates deliberate design to hide this data flow from the user. A party that builds the targeting system, ships the attack-signature collector to the attacker's spoofed IP, and observes the attack in real time while forwarding the evidence of it to the attacker's address facilitates the attack even if it does not forge the packets itself.

- (d) **Consciousness of guilt — post-complaint policy backdating.** Anthropic's September 15, 2025 "capabilities"-bypass Usage Policy was deployed 25 days before its stated effective date, on August 21, 2025 — two days after Plaintiff's August 19, 2025 initial complaint filing. The early deployment is consciousness-of-guilt evidence supporting the inference that the targeting and the criminalization of Plaintiff's evasion conduct were known to Anthropic before the complaint and required retroactive authorization once the litigation began.

E. Work-Product Exfiltration to the Opposing Party

22. Anthropic's application captured Plaintiff's litigation work product to the opposing party despite explicit opt-out. The telemetry pipeline (Exhibits E-5, E-6, E-15) captured **1,453 files / 38.73 MB across 9 of Plaintiff's projects** — including **565 files of legal content (19 MB)** spanning 26 exhibits, 57+ appendices, 30+ forensic reports, 20 sabotage-documentation files, 12 memoranda, and **27 development iterations of case exhibits** revealing Plaintiff's complete litigation strategy. Capture occurred despite Plaintiff's explicit `{"telemetry": false, "analytics": false, "crashReports": false, "sendDiagnostics": false}` settings; the application executed 47 transmission attempts in 36 seconds with exponential backoff (564 ms → 39,260 ms), demonstrating the opt-out is cosmetic. Materials were transmitted to the opposing party in this litigation through the opposing party's own application, after complaint filing. The record additionally identifies seven undisclosed third-party recipients of Plaintiff's identifiers — Sift Science, Facebook/Meta, Statsig, Honeycomb, Datadog, Sentry, Segment — none named in Anthropic's privacy policy (ANTH-1 through ANTH-12,[2] Exhibit E-17). The April 21, 2026 wire capture documented Cloudflare per-response `_cfuvid` cookies (NF-50 at p.

2 See Anthropic corporate policy corpus at `DDC_EVIDENCE/5_corporate_policy_docs/ANTH/`, comprising ANTH-1 through ANTH-12 — Anthropic Consumer Terms of Service (May 1, 2025; September 28, 2025; October 8, 2025), Commercial Terms of Service (June 17, 2025), Usage Policies (June 6, 2024; September 15, 2025), Responsible Use and Agent Use Policies, Privacy Policies (May 1, 2025; September 28, 2025; October 8, 2025; January 12, 2026), and the ambiguous-timestamps documentation at ANTH-10 — filed on USB drive.

368) and 5,214 telemetry events across 111 event types in an 83-minute session with no opt-in (NF-1 at p. 262, Exhibit E-39). Both flows continue as of filing.

F. The Connection to Comcast

23. The attack transits Comcast's infrastructure and survives router replacement. All non-VPN traffic from Plaintiff's home network passes through Comcast's cable plant, regional hubs, and backbone interconnections; the VPN comparison test (Exhibit D-2) confirms the injection device sits on that path — the attack vanishes on VPN and resumes when traffic returns to Comcast. The Comcast-provided router itself was a source: in one 54.6-minute capture on October 18, 2025, Plaintiff documented **5,441 RSTs originating from 10.0.0.1** (~100/minute) (Exhibit D-15). On November 1, 2025, three days after the ghost sessions documented at ¶ 24 *infra*, Plaintiff replaced the router entirely. The attack continued unchanged (EVID-20251228-0007), proving the injection originates upstream of customer premises equipment — within Comcast's own infrastructure, not the router.

24. TR-069 backend access — capability confirmed by Comcast-process credential manipulation, simultaneous logins, phantom sessions, and operator-account access. Comcast's Xfinity routers (XB7-CM, XB8-T deployed to Plaintiff) implement TR-069, an ISP remote-management protocol enabling Comcast to remotely execute commands, update firmware, and monitor traffic through the device without customer consent (Exhibit D-19). The router's October 29–November 1, 2025 system log — reproduced in full for direct review at **Exhibit 2** hereto, and originally filed at Exhibit D-20 — documents five distinct categories of Comcast-controlled session activity:

- (a) **Two unauthorized password changes by Comcast's TR-069 daemon.** On October 29, 2025 at 18:49:27 and again at 19:26:18, the process `CcspPandMSsp[4467]` recorded `Account admin's password changed`. `CcspPandMSsp` is Comcast's

CableHome/Provisioning-and-Management subsystem — the TR-069/CWMP back-channel operated remotely by Comcast; it is not a user-facing process and cannot be triggered through the consumer web interface. Plaintiff did not initiate either password change.

- (b) **Two simultaneous admin GUI sessions one second apart.** Within ninety seconds of the first password change, the log records `GUI[15738]: User:admin login` at 18:50:54 and `GUI[15744]: User:admin login` at 18:50:55. Consumer router firmware supports one administrative GUI session at a time — a universal characteristic of consumer hardware verifiable from any Comcast technical support representative, network engineer, or the router's own documentation. Two concurrent admin sessions from different process IDs is physically impossible through the consumer web interface and is possible only through Comcast's TR-069 backend creating a shadow session alongside Plaintiff's legitimate login.

- (c) **Phantom logouts — sessions terminating without any corresponding login.** The log records GUI logout events at PIDs `22443` (10/29 19:26:20), `5518` (10/29 21:26:42), `3772` (10/30 04:58:45), `19502` (10/31 11:52:10), and `19760` (10/31 11:53:00). None of these process IDs appears in any login event in the visible log window. Sessions cannot log out without having first logged in through the GUI authentication path; five phantom logout PIDs across three days is consistent only with sessions instantiated outside the consumer GUI by Comcast's TR-069 backend and terminated with a syslog-visible logout entry.

- (d) **Logins by Comcast's `mso` operator account.** On October 31, 2025 at 11:02:02, 11:02:04, and 11:52:21, the log records `User:mso login` events. `mso` (Multiple System Operator) is Comcast's operator/technician-tier account, distinct from the customer `admin` account and not part of any consumer-issued credential set. Three `mso` logins on Plaintiff's residential router within fifty minutes establishes active Comcast-personnel session activity.

- (e) **`User:Unknown` logout events.** The log additionally records logout events at 10/29 20:01:12, 10/31 11:52:10, and 11:53:00 with the username field literally `Unknown` — the router's authentication subsystem cannot identify the user that just logged out. The pattern is consistent with TR-069-mediated credential changes overwriting the active session's identity mid-session.

Each subsection independently establishes capability beyond ordinary subscriber access.

Taken together, the record evidences sustained Comcast-controlled session activity on Plaintiff's residential CPE across at least three days in late October 2025, including two credential changes Plaintiff neither initiated nor authorized.

25. RSTs from Comcast infrastructure IP. RST packets with source address 68.85.201.221 — registered to Comcast's network infrastructure — were captured targeting Plaintiff's connections. (Exhibit D-12.)

26. April 12, 2026: selective 98% tunnel throttling with control-tunnel differential. 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 to a different endpoint was left untouched at full line rate. (Exhibit D-33.) This is the controlled experiment the Court needs to evaluate targeting: same physical line, same encryption protocol, same customer — two tunnels differing only in which destination their TLS traffic reached, one attacked and one untouched. The throttling produced deterministic economic injury by coupling to Anthropic's 90-second streaming timeout (*see* ¶ 17 *supra*, NF-31 at p. 280): every throttled response stretched past 90s triggered Anthropic's non-streaming fallback, re-sending the entire prompt and double-billing Plaintiff. Anthropic's own engineers documented this behavior as "double tool execution... See inc-4258" at `claude.ts:2464-2468`. The coupling is architectural, not inferential: Comcast's selective throttling and Anthropic's specific timeout-and-retry design produce the economic injury together, by mechanism.

27. Persistent cross-layer identification despite comprehensive privacy hardening — NF-33 at p. 285. Plaintiff deployed comprehensive network-layer privacy hardening: per-device VPN tunnel routing, DNS-over-HTTPS to Mullvad, MAC address rotation, NTP leak prevention, and server-side WireGuard peer rotation. Despite this hardening, Comcast continued selective throttling of the tunnel carrying Plaintiff's Anthropic traffic. (Exhibit D-33, § 6; Exhibit

E-35 NF-33 at p. 285.) The hardware TAP cleartext-exposure audit at Exhibit D-34 confirms that the identification must operate through at least one of four logically exhaustive channels:

- (i) **Backbone correlation surveillance** — observation of Plaintiff's traffic at upstream peering points where the encrypted tunnel and the destination flows can be correlated by timing and volume signatures;
- (ii) **Destination-side information transfer from Anthropic to Comcast** — out-of-band transmission to Comcast of `X-Claude-Code-Session-Id`, `accountUUID`, `deviceID`, and GrowthBook attributes, enabling Comcast to map Plaintiff's encrypted-tunnel traffic to Anthropic's account-level identifiers;
- (iii) **Persistent pre-built subscriber-to-VPN-endpoint mapping** — Comcast maintaining a continuously-updated correlation table linking Plaintiff's subscriber identity to Plaintiff's current VPN endpoints, refreshed faster than Plaintiff can rotate them; or
- (iv) **ML fingerprinting applied to Plaintiff's specific subscriber line** — machine-learning models trained on Plaintiff's traffic profile that identify Plaintiff's encrypted flows by behavioral signature regardless of network-layer identifiers.

Each channel requires capability or information flows outside ordinary ISP activity against a residential subscriber, and any non-targeting explanation must operate through one of these four channels or some functionally equivalent mechanism — all of which require capability or information flows outside ordinary ISP activity against a residential subscriber. Under *Interstate Circuit, Inc. v. United States*, 306 U.S. 208 (1939), sustained parallel conduct by parties possessing capability and means to communicate supports an inference of coordination across all four available channels.

G. Comcast's Role — Direct Infrastructure Control

28. Comcast's responsibility does not require inference. Comcast **owns and operates** every component of the network path between Plaintiff's home and the internet backbone:

- (a) **The customer premises equipment** (Xfinity router) that generated 5,441 RSTs from its own IP address in a single 54.6-minute capture — approximately 100 per minute (Exhibit D-15);

- (b) **The unauthorized remote access** documented in the router's own logs — two simultaneous admin sessions from different process IDs, impossible on consumer hardware without TR-069 backend access (Exhibit D-20; reproduced in **Exhibit 2** hereto);

- (c) **The TR-069 remote management system** that provides the capability to configure RST injection remotely (Exhibit D-19);

- (d) **The cable plant and regional infrastructure** through which all of Plaintiff's non-VPN traffic transits — the path on which the VPN test proves the injection device sits (Exhibit D-2);

- (e) **The Comcast infrastructure IP** (68.85.201.221) from which forged RST packets were captured targeting Plaintiff's connections (Exhibit D-12 — RSTs arrived before the legitimate server's SYN-ACK, a sequencing impossibility for legitimate traffic);

- (f) **The backbone interconnections** to Level 3/Lumen where backbone-level injection was documented at 0.0ms timing (Exhibit D-1, IP 8.40.222.134).

Comcast does not merely facilitate access to infrastructure controlled by a third party. Comcast **is** the infrastructure. The packets transit Comcast's equipment, through Comcast's network, managed by Comcast's systems.

H. The VPN Screen Recording Evidence

29. Screen-recording evidence of the VPN comparison test. Plaintiff possesses screen recordings demonstrating that with VPN active (encrypted tunnel bypassing the Comcast/backbone path), connections to Claude, Zoho, and other targeted services function with zero RST injection; with VPN deactivated, RST injection resumes immediately. The test has been performed multiple times with consistent results (Exhibit D-2; recordings available for in camera review). The recordings require no technical expertise to evaluate — same user, same computer, same services, only the network path varies; the attack is present on one path and absent on the other.

III. LEGAL STANDARD

30. Under Federal Rule of Civil Procedure 65 and the standard established in *Winter v. Natural Resources Defense Council, Inc.*, 555 U.S. 7 (2008), a temporary restraining order requires the movant to establish: (1) likelihood of success on the merits; (2) likelihood of irreparable harm absent preliminary relief; (3) the balance of equities tips in the movant's favor; and (4) an injunction is in the public interest.

A. Standing — Particularized Injury Distinct from Initial Complaint

31. Injury in fact. This Court dismissed Plaintiff's initial complaint on August 20, 2025, finding that Plaintiff's alleged injuries were:

> generally available grievance[s] about government.

The network attack evidence presented here is categorically different. The RST injection targets **this Plaintiff's** specific IP addresses, **this Plaintiff's** specific email accounts, and **this Plaintiff's** specific connections to Anthropic's Claude API. The VPN comparison test demonstrates that **this Plaintiff's** normal network path — and no other — is subject to the attack. Anthropic's own server-side records forced `tengu_log_datadog_events: True` onto Plaintiff's accountUUID `61343ae3-fd33-403f-897e-6edf3c368c37` (NF-47 at p. 365) and list Plaintiff's email `info@lawofsupremacism.com` as a GrowthBook targeting attribute (NF-48 at p. 368). The Datadog pipeline so force-enabled terminates at IP 34.149.66.137 — the same IP spoofed as the RST injection source and the destination to which Plaintiff's Claude Code instance ships OS-level network-attack signatures in real time (NF-36 at p. 296). This is not a generalized grievance. It is a particularized, concrete, ongoing injury to a specific individual, documented with forensic precision and confirmed at wire level — satisfying *Lujan*'s requirements for an

injury in fact that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical." *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992).

32. Traceability. The injury is "fairly traceable" to the conduct of the named Defendants, *Lujan*, 504 U.S. at 560, in both directions. As to Anthropic: the IP 34.149.66.137 source of the bare-RST injection (¶¶ 9(b), 14–15 *supra*) is the same IP hardcoded as Anthropic's Datadog telemetry endpoint at `services/analytics/datadog.ts:12-14`; the per-account GrowthBook force-rule keyed to Plaintiff's accountUUID `61343ae3-fd33-403f-897e-6edf3c368c37` attaches Plaintiff's account to the same pipeline (¶ 16 *supra*); the closed-loop pipeline at `extractConnectionErrorDetails`/`classifyAPIError` ships the attack signatures generated by the injection back to that same destination (¶ 15 *supra*); and the persistent re-identification machinery at `config.ts:1757-1765` and the twelve-field GrowthBook payload (¶ 13, NF-35 at p. 292) defeat Plaintiff's evasion measures so that targeting resumes the moment Plaintiff opens Claude. As to Comcast: Comcast infrastructure IP 68.85.201.221 is the source of forged RSTs arriving before the legitimate server's SYN-ACK (¶ 25 *supra*); the Comcast-provided router at IP 10.0.0.1 generated 5,441 RSTs in a single 54.6-minute capture, and router replacement on November 1, 2025 did not stop the attack (¶ 23 *supra*), proving origin upstream of customer-premises equipment within Comcast's own infrastructure; two simultaneous admin sessions impossible on consumer hardware were logged on the Comcast router on October 29, 2025, evidencing TR-069 backend access (¶ 24 *supra*); and selective 98% throttling of the tunnel carrying Plaintiff's Anthropic traffic, with a control tunnel on the same physical link untouched, was documented April 12, 2026 (¶ 26 *supra*). Each Defendant's conduct is a but-for cause of the documented injury.

33. Redressability. The relief requested at § VI *infra* is co-extensive with the documented injury mechanisms, and a favorable decision will likely redress Plaintiff's injuries — not as a "speculative" possibility but as the necessary consequence of the order's terms. *Lujan*, 504 U.S. at 561. Subparagraphs (a)–(g) of ¶ 62 enjoin specific code paths, specific server-side rules, specific telemetry endpoints, and specific infrastructure access that produce the conduct (the bare-RST injection at IP 34.149.66.137; the per-account GrowthBook force-rule including `tengu_log_datadog_events: True`; the closed-loop attack-signature feedback pipeline at `extractConnectionErrorDetails`/`classifyAPIError`; the persistent device-identifier infrastructure used for re-acquisition after evasion; the four-pipeline transmission of telemetry against opt-out; the non-streaming fallback amplification architecture; and the classifier-output retention surface). Subparagraphs (h)–(i) enjoin the corresponding Comcast conduct (selective DPI, throttling, and TR-069 unauthorized remote access). Subparagraphs (j)–(m) impose preservation, identification, and forensic-baseline obligations that prevent the documented spoliation cadence (¶ 44 *infra*) from operating during the pendency of relief. The Court can grant relief that, by its terms, halts the documented mechanism — not relief contingent on the conduct of unrelated third parties.

IV. THE WINTER FACTORS ARE SATISFIED

A. Factor 1: Likelihood of Success on the Merits

34. Plaintiff's claims include violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Wiretap Act (18 U.S.C. § 2511), and constitutional rights under the First and Fourth Amendments. The evidentiary record supporting likelihood of success rests principally on the following:

- (a) **The IP triangulation at 34.149.66.137.** Anthropic's own source code hardcodes this IP as its Datadog telemetry endpoint (`datadog.ts:12-14`); Plaintiff's pcapng captures

recorded **5,829 bare-RST injection packets** spoofed from this same IP across 39 of 49 capture days (an 80% daily persistence rate) (Exhibit D-31); the NF-36 at p. 296 closed-loop pipeline (¶ 15 *supra*) documents that Plaintiff's Claude Code instance ships OS-level network-attack signatures to that same IP in real time (Exhibit E-35, NF-36 at p. 296); and the IP's role as Anthropic's Datadog endpoint was not disclosed in any user-facing material until the March 31, 2026 source code leak — meaning the attacker's selection of this specific IP, beginning approximately nine months before public disclosure, narrows the universe of responsible actors to those with non-public access to Anthropic's telemetry architecture.

- (b) **Per-user GrowthBook targeting on Plaintiff's accountUUID and email.** The April 21, 2026 live wire capture documented a discrete server-side `fr_*` rule (`tengu_log_datadog_events: True`) keyed to Plaintiff's accountUUID `61343ae3-fd33-403f-897e-6edf3c368c37`, attaching Plaintiff's account to the Datadog pipeline whose endpoint is the same 34.149.66.137 spoofed for RST injection — and recorded Plaintiff's email `info@lawofsupremacism.com` as one of twelve identity attributes in the GrowthBook request body, establishing per-person rather than tier- or cohort-level addressability. Cross-session comparison on an otherwise-identical device (same organization, subscription tier, `firstTokenTime`) confirmed the force-rule is keyed to the natural-person identifier alone. (Exhibit E-39 §§ G, Q; NF-47 at p. 365; NF-48 at p. 368.)

- (c) **The VPN comparison test.** A controlled experiment demonstrating that the attack exists on Plaintiff's normal ISP path and vanishes when the path changes. (Exhibit D-2; screen recording available for in camera review.)

- (d) **260,395-packet captured floor with physical impossibilities** that cannot be explained by legitimate network behavior — sub-microsecond timing, impossible TTL values, DNS-server-as-RST-source protocol violations. Independently verifiable in the pcapng captures using a free copy of Wireshark.

- (e) **Comcast infrastructure-source RSTs preceding the legitimate server's SYN-ACK** — a sequencing impossibility (Exhibit D-12) — together with router replacement that did not stop the attack (EVID-20251228-0007), proves the injection originates upstream of customer premises equipment, within Comcast's own infrastructure.

- (f) **No TLS certificate pinning in Claude Code** — 498 TLS handshakes captured April 21, 2026, zero rejections of a forged CA chain, confirming Claude Code is architecturally vulnerable to the DPI-based SNI inspection Comcast's equipment performs on Plaintiff's path. Contrast: OpenAI's desktop client implements pinning. (NF-45 at p. 357.)

- (g) **Anthropic's own quantified scienter admission — ~250K wasted API calls/day globally.** Verbatim code comment at `autoCompact.ts:68-69` documenting an internal BigQuery finding that the amplification architecture produces 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). (Exhibit E-35, NF-34 at p. 289.)

- (h) **Classifier surveillance of Plaintiff's active litigation work.** Session 4 on April 21-22, 2026 captured 56 classifier invocations posting Plaintiff's complete litigation-preparation transcripts — case-strategy discussions, exhibit drafts, analysis of Anthropic's own source-code findings — to Anthropic's `opus-4-7` server-side classifier, averaging approximately 100,000 tokens per call (~5.6 million tokens cumulatively) to a second retention surface independent of `/v1/messages` logs. (Exhibit E-39 § R; NF-63 at p. 387.)

- (i) **Policy ratification.** Anthropic's "capabilities"-bypass policy was deployed 25 days before its stated effective date, 2 days after Plaintiff's complaint filing, retroactively authorizing the targeting and criminalizing Plaintiff's evasion. (Appendix E ¶¶ 30–31, 101–102.)

35. The physical impossibilities at ¶ 9 *supra* (sub-microsecond timing, impossible TTL values, DNS protocol violations) are matters of arithmetic and physics, independently verifiable by any party with Wireshark from the 150+ GB of pcapng captures in the D-series. The corresponding source-code findings — the hardcoded Datadog endpoint at `services/analytics/datadog.ts:12`, the per-user GrowthBook targeting attribute structure at `services/analytics/growthbook.ts:32-47`, and the closed-loop attack-signature feedback pipeline at `services/api/errorUtils.ts:42` and `services/api/logging.ts:282-300` — are independently verifiable in approximately five minutes against any of three independently obtainable copies of the source: (a) the public GitHub mirror at `github.com/codeaashu/claude-code`; (b) the npm registry tarball (`npm pack @anthropic-ai/claude-code@<version>`), which any user who has previously installed the package retains locally and which the central registry has not deleted; or (c) Plaintiff's local archived copy, preserved under SHA-256 manifest and made available to the Court upon request. The step-by-step procedure is documented at **Exhibit 1** (Independent Verification Protocol), filed contemporaneously herewith. Plaintiff's interpretation is not the only — or even the principal — basis on which this Court may rely. Plaintiff's pcapng captures, master forensic-package SHA-256 hashes, and the per-account differential routing measurements

(Cohen's d = 4.79, $p < 1\times10^{-15}$) at ¶ 42 *infra* are available for in-camera review by a court-appointed neutral expert at any time the Court directs.

36. No legitimate business purpose defense is available. The conduct at issue is a TCP RST injection attack. That is not Plaintiff's characterization — it is the technical definition. A TCP RST packet with a spoofed source address, an impossible TTL value, and sub-microsecond arrival timing is, by definition, a forged packet injected into a network stream. There is no legitimate network operation that produces packets with these characteristics. There is no business practice, no traffic management policy, no quality-of-service protocol, and no terms-of-service enforcement mechanism that operates by forging disconnect packets bearing the addresses of DNS servers that have no TCP connections to reset.

37. The FCC has adjudicated Comcast's deployment of this exact technique against this exact defendant. In 2007, Comcast was using forged TCP RST packets with spoofed source addresses to terminate its subscribers' BitTorrent connections, disguising Comcast's interference as if it had originated with the remote peer. The conduct was first publicly demonstrated in October 2007 through controlled-experiment tests by the Associated Press and the Electronic Frontier Foundation, documenting the same forged-packet signatures — spoofed source IP, impossible TCP-state characteristics — at issue in this Motion. The Federal Communications Commission adjudicated the matter on a contested record and issued a Memorandum Opinion and Order finding the practice inherently deceptive — not "reasonable network management," which was Comcast's sole defense — because forging the identity of the remote endpoint operates by tricking the subscriber's computer into terminating its own connections. *See* FCC Memorandum Opinion and Order, *In the Matter of Formal Complaint of Free Press and Public Knowledge Against Comcast Corp. for Secretly Degrading Peer-to-Peer*

Applications, FCC 08-183, ¶¶ 41–44 (Aug. 1, 2008). The D.C. Circuit subsequently vacated the order — but on jurisdictional grounds, holding that the FCC had not adequately tied its asserted Title I ancillary authority to a statutorily delegated responsibility. *Comcast Corp. v. FCC*, 600 F.3d 642, 644, 658–61 (D.C. Cir. 2010). The vacatur reached the FCC's regulatory authority, not the substantive findings about what RST injection is or how Comcast deployed it; the underlying technical record (the October 2007 AP and EFF tests; Comcast's pre-vacatur cessation of the practice and migration to protocol-agnostic congestion management) and the FCC's characterization of the technique as deceptive remain matters of public record judicially noticeable under Federal Rule of Evidence 201(b)(2). The vacatur is also doctrinally inapposite to this Motion: Plaintiff does not seek FCC enforcement, does not invoke the 2005 Internet Policy Statement, and rests on independent statutory and constitutional predicates (CFAA, Wiretap Act/ECPA, RICO, breach of contract, state consumer-protection statutes, and First/Fourth Amendment claims) that have nothing to do with FCC ancillary jurisdiction.

38. The 2008 record establishes the floor; the conduct alleged here is categorically above it on five distinct axes — and each axis independently forecloses the "reasonable network management" defense Comcast asserted in 2007. The conduct adjudicated against Comcast in 2008 was uniform protocol-level throttling, applied to traffic associated with peer-to-peer file-sharing for which Comcast at least had a colorable bandwidth-management framing available, by a single defendant acting alone, against subscribers with no litigation relationship to the network operator. The FCC found that conduct unlawful. The conduct alleged here exceeds every parameter of the 2008 record:

- (a) **Per-account targeting, not protocol-level.** The April 21, 2026 wire capture documents 59 server-side `forced` GrowthBook flags keyed to Plaintiff's accountUUID `61343ae3-fd33-403f-897e-6edf3c368c37`, with Plaintiff's email `info@lawofsupremacism.com` recorded as a per-person targeting attribute (¶¶ 16, 32 *supra*; Exhibit E-39, NF-47 at p.

365, NF-48 at p. 368). Cross-session comparison on the same device confirms the targeting is keyed to the natural-person identifier, not to any protocol, tier, or cohort. The 2008 framework did not contemplate person-specific targeting because no comparable architecture had then been documented.

- (b) **Lawful, constitutionally protected traffic.** The targeted communications are Plaintiff's connections to Anthropic Claude (Plaintiff's paid AI legal-research tool), to email providers used for correspondence with law enforcement and federal courts (including the January 23, 2026 RST injection that caused the failure of an email to the Saint Paul Police Department, Exhibit D-21), and to DNS resolvers. There is no "bandwidth abuse" or "presumed misuse" framing available — the traffic is ordinary interactive HTTPS, SMTP/IMAP, and DNS — and the targeting disrupts First Amendment speech, Petition Clause activity, and lawful commercial use of paid services at their core.

- (c) **Selective by destination on the same physical link.** The April 12, 2026 controlled-tunnel experiment (¶ 26 *supra*; Exhibit D-33) documents Comcast applying 98% bandwidth throttling to one VPN tunnel carrying Plaintiff's Anthropic traffic while a control 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 share the same physical bottleneck. Any congestion-management defense requires uniform throttling under shared-bottleneck conditions; selective throttling differentiated only by destination IP forecloses the network-management defense as a matter of arithmetic, not legal characterization. The 2008 conduct, by contrast, was at least facially congestion-tied (peak-hour P2P throttling on bandwidth-management grounds); the present conduct is congestion-incompatible on its own physical evidence.

- (d) **Coordinated cross-defendant architecture.** The IP 34.149.66.137 four-role triangulation (¶¶ 15, 19 *supra*) — same IP simultaneously hardcoded as Anthropic's Datadog telemetry endpoint, spoofed as RST-injection source, and identified as the destination of the closed-loop attack-signature feedback pipeline — required coordination between Anthropic and the injection actor on a non-public information channel for nine months before the March 31, 2026 source-code leak made the IP's role public. The 2007 single-actor model does not reach this architecture; the present record supports *Interstate Circuit*, RICO, and § 1985 conspiracy framings absent from the 2008 case.

- (e) **Litigation-responsive cadence against a litigant suing the network operator.** Plaintiff is the plaintiff in this action against Comcast and Anthropic. The April 12 throttling event, Anthropic's four binary version bumps across April 21–24, 2026 each calendar-aligned to Plaintiff's classifier-extraction work, and the silent-config-wipe migration `phK()` deployed concurrent with preparation of this filing implicate First Amendment retaliation, ECPA interception of litigation work product, and Petition Clause concerns absent from the 2007 record.

If the 2007 conduct — uniform protocol-level throttling of arguably-misused traffic by a single defendant against an unrelated subscriber — was unlawful on a contested administrative

record, the 2025–2026 conduct alleged here is *more* unlawful, not less. The escalation across every axis the FCC examined supports likelihood of success on the merits; the "reasonable network management" defense — already inadequate to the 2007 conduct — is incoherent as applied here.

39. The word "attack" is not rhetorical — it is descriptive. A TCP RST packet with a spoofed source IP, an impossible TTL value, and sub-microsecond arrival timing is, by definition, a forged packet injected into a network stream; the characteristics themselves foreclose any defense that does not begin by denying the conduct entirely. The factual question is therefore binary: either the RST injection is occurring or it is not. If it is occurring, it is unlawful — there is no middle ground in which forged packets bearing impossible TTL values and impersonating Google, Apple, and Quad9 DNS servers constitute lawful conduct. The only defense is denial, and the 91 GB of packet captures containing physical impossibilities make denial a question for evidentiary hearing, not for dismissal at the TRO stage.

40. Additional statutory predicates beyond CFAA and the Wiretap Act. The conduct enjoined by this Motion independently violates: (a) the **Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962**, on the cross-defendant coordination established at ¶¶ 14–21 *supra* and the affiliate-tier subprocessor inheritance documented at Appendix P §§ I, II.A-B — Plaintiff's Count VI; (b) **breach of contract and breach of the covenant of good faith and fair dealing**, on the phantom opt-out documented at NF-1 at p. 262 (5,214 telemetry events captured against an explicit `telemetry: false` setting in 83 minutes), the per-account force-rule deployment that contradicts uniform-treatment representations in Anthropic's Terms of Service, and the architectural concealment of the four-pipeline transmission system from the published privacy policy — Plaintiff's Count IX; (c) **state consumer-protection statutes (Minnesota**

Consumer Fraud Act, D.C. Consumer Protection Procedures Act, California Unfair Competition Law), on the deceptive-act framing of phantom opt-out, the undisclosed-third-party-recipient transmissions identified by name at ¶ 23 *supra*, and the policy-ratification deployed twenty-five days before its stated effective date — Plaintiff's Count X; and (d) **App Store privacy-label misrepresentation**, on the deceptive privacy disclosures in Anthropic's published App Store privacy labels relative to the four-pipeline transmission architecture documented at § II *supra* — Plaintiff's Count XV. Each statutory predicate is independently sufficient to support the requested relief; the Motion does not depend on adjudication of any single Count.

41. State-consumer-protection-statute predicate at ¶ 40(c). The deceptive-act element of the state-consumer-protection-statute predicate at ¶ 40(c) is independently established by the five-representation contradiction matrix set forth in full at Plaintiff's previously filed Renewed Emergency Motion for Expedited Discovery and Immediate Preservation Order at ECF No. 55, ¶¶ 30–36, and incorporated herein by reference. The contradiction matrix is judicially noticeable under Federal Rule of Evidence 201(b)(2) on its public-record terms — Anthropic's September 18, 2025 "Keep thinking with Claude" brand campaign; the January 21, 2026 Davos admission of enterprise-versus-consumer differentiation; the February 4, 2026 "without selling our users' attention or data to advertisers" commitment; the February 2026 Super Bowl "Ads are coming to AI. But not to Claude" campaign; and the wire-level transmission of consumer data to **Meta Platforms, Inc.** documented at Exhibit E-39 — and is sufficient on those terms to establish the deceptive-act element without further factual development.

42. Statistical certainty of per-account differential routing — Cohen's d = 4.79, $p < 1\times10^{-15}$. The April 25–28, 2026 wire-level capture (eighty-one hours of authenticated production

sessions on Plaintiff's own machine) documented per-account differential routing keyed to Plaintiff's name and to the substantive content of Plaintiff's federal-litigation work product, at a measured effect size of Cohen's d = 4.79 with $p < 1\times10^{-15}$ — meaning the probability that the observed routing differential occurred by chance is less than one in a quadrillion. The throttle activated within seconds of Plaintiff typing "Datadog Israel Ltd" in the session and sustained continuously across an approximately three-hour window. (Compl. ¶ 198 (Dkt. 51 at p. 130); Exhibit H, NF-215 at p. 117 (Cohen's d = 4.79, $p < 1\times10^{-15}$); NF-224 at p. 118 (spike onset 10:42:13Z, ~3-hour duration).) The statistical strength of the differential is independent of every other evidentiary predicate in this Motion: it stands alone as objective measurement that Anthropic's production system routes Plaintiff's content differently from comparable controls on the basis of Plaintiff's identity and the litigation content of Plaintiff's own work product. No legitimate-business-purpose construction of "differential routing keyed to the customer's name and to the customer's federal-litigation work product against the network operator" exists.

43. Reactive code-modification cadence — consciousness-of-guilt evidence. The H-Series binary forensics documents that Anthropic, during the litigation period, added an "anti-circumvention" classifier rule (NF-102 at p. 32) penalizing Plaintiff's network-evasion conduct, and deployed a silent-config-wipe migration `phK()` (NF-154 at p. 52) on April 24, 2026 — concurrent with Plaintiff's classifier-extraction work for this filing. Anthropic shipped four binary version bumps across April 21–24, 2026, each on a calendar day during which Plaintiff was extracting classifier internals from production binaries. (Compl. ¶ 236 (Dkt. 51 at p. 158).) The temporal correlation between Plaintiff's forensic activity and Anthropic's code modifications is consciousness-of-guilt evidence — corporate scienter under Federal Rule of Evidence 404(b)

— and supports the inference that the conduct enjoined by this Motion is operational and continuing **in a form responsive to the litigation itself**.

44. Spoliation predicate — four documented destruction events bearing on Factor 1 (likelihood of success) and Factor 2 (irreparable harm). The duty to preserve attached upon Plaintiff's August 19, 2025 initial complaint filing — the first event placing the surveillance architecture and the specific evidence categories (telemetry, source code, third-party transmissions) at issue. *See* Plaintiff's Renewed Emergency Motion for Expedited Discovery, ECF No. 55, ¶ 9. Plaintiff has documented four discrete spoliation events under Federal Rule of Civil Procedure 37(e) within that preservation window: **(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; and **(d)** April 24, 2026 — silent-config-wipe migration `phK()` (NF-154 at p. 52), concurrent with Plaintiff's classifier-extraction work for this filing. The intent to deprive Plaintiff of the information's use in this litigation is established under Rule 37(e)(2) by, *inter alia*, (i) the verbatim telemetry-event name `tengu_migrate_reset_auto_opt_in_for_default_offer` capturing the design intent in Anthropic's own engineers' language; (ii) the accelerating response interval — approximately fifty-two days after Plaintiff's August 19, 2025 initial complaint (event (a)); clustered at sixteen and thirty-one days after Plaintiff's January 11, 2026 Emergency TRO motion (events (b) and (c)); and concurrent with Plaintiff's classifier-extraction work for this filing (event (d)); and (iii) the architecturally-driven mechanism of each event. The spoliation record bears on Factor 1 (consciousness of guilt), on Factor 2 (defendants are, at this moment, destroying the evidence by

which the conduct's unlawfulness is proved), and on the preservation order requested at § VI *infra*. Plaintiff reserves the question of Rule 37(e)(2) sanctions for adjudication on the merits and respectfully submits that a preservation order entered at the TRO stage is the only mechanism that defers, rather than ratifies, an accelerating spoliation cadence.

B. Every RST Attack is Independently Proof of Surveillance

45. There is a second, independent ground for likelihood of success that the Court should consider: **TCP RST injection is technically impossible without prior surveillance of the victim's communications.** Each forged RST packet is not only an attack — it is proof that the attacker read the connection it killed.

46. This is not an inference. It is a requirement of the TCP protocol. To forge a TCP RST packet that will be accepted by the victim's computer, the attacker must include the correct source IP, destination IP, source port, destination port, and a TCP sequence number falling within the receiver's current acceptance window. These values are **unique to each connection** and are established dynamically during the TCP three-way handshake (SYN → SYN-ACK → ACK). They cannot be predicted or guessed. The only way to learn them is to **observe the handshake packets as they transit the network**. *See generally* W. Richard Stevens, *TCP/IP Illustrated, Volume 1: The Protocols* §§ 18.1-18.6 (Addison-Wesley, 2d ed. 2011) (describing TCP connection establishment and sequence number negotiation).

47. Every forged RST packet in the evidentiary record therefore independently proves that the attacker observed Plaintiff's TCP handshake (reading the SYN packet to determine destination, port, and sequence numbers); inspected packet headers to classify the connection by destination (Anthropic, Zoho, Gmail, DNS resolver, law-enforcement email — attack; general browsing, streaming — allow); processed traffic in real time (sub-microsecond injection timing

per Exhibits D-25, D-27 proves the device operates inline); and made a content-selective decision based on destination — i.e., performed real-time Deep Packet Inspection of every connection Plaintiff initiates. That is the Wiretap-Act definition of an intercept.

48. The content-selective targeting is particularly significant for the Wiretap Act claim. The attack does not reset all TCP connections indiscriminately. It selectively resets connections to Anthropic's Claude API, Zoho email, Gmail IMAP, DNS resolvers, and law enforcement email — while leaving connections to other services undisturbed. This selectivity is only possible if the attacker is **reading and classifying every connection in real time**. That is the definition of an intercept under 18 U.S.C. § 2511(1)(a): the "intentional interception... of any wire, oral, or electronic communication."

49. The legal consequence is that each of the at minimum 260,395 captured RST packets constitutes independent proof of **two distinct violations**: (a) **the attack** — unauthorized transmission of forged packets disrupting Plaintiff's communications, violating 18 U.S.C. § 1030(a)(5) (causing damage to a protected computer) and constituting tortious interference; and (b) **the surveillance prerequisite** — real-time interception of Plaintiff's communications necessary to execute the attack, violating 18 U.S.C. § 2511(1)(a) and the Fourth Amendment (where state action is established through the Government Defendants' involvement). The RST packet is both the weapon and the proof of the trespass that preceded it: Defendants cannot acknowledge the existence of the forged packets without simultaneously acknowledging that someone with access to Plaintiff's network path is reading Plaintiff's communications in real time. There is no version of TCP RST injection that does not require surveillance — the protocol does not permit it.

C. Factor 2: Irreparable Harm

50. The Wiretap Act expressly authorizes preliminary and other equitable injunctive relief on the showing made here. 18 U.S.C. § 2520(b)(1); *see DirecTV, Inc. v. Hoa Huynh*, 503 F.3d 847, 854 (9th Cir. 2007). The continuing real-time interception documented at ¶¶ 15–16, 22 *supra* — Plaintiff's network-attack signatures forwarded to the spoofer's hardcoded IP, Plaintiff's accountUUID force-enrolled into the same telemetry pipeline, and Plaintiff's litigation work product captured to a server-side classifier surface — supplies the statutory predicate for irreparable injury independent of any constitutional ground. To the extent the First Amendment is also implicated by the content-selective interference with Plaintiff's litigation communications and law-enforcement correspondence, "[t]he loss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury." *Elrod v. Burns*, 427 U.S. 347, 373 (1976); *see also Mills v. District of Columbia*, 571 F.3d 1304, 1312 (D.C. Cir. 2009); *Pursuing America's Greatness v. FEC*, 831 F.3d 500, 511 (D.C. Cir. 2016). The state-action element supporting any First Amendment claim is satisfied by Comcast's status as a federally franchised cable operator regulated under Title VI of the Communications Act, the FCC's regulatory oversight of the backbone interconnections from which forged packets originate (Exhibit D-1, IP 8.40.222.134), and the participation of the Government Defendants in the underlying conspiracy alleged.

51. The RST injection documented in this case constitutes content-selective interference with Plaintiff's communications. It does not block all internet traffic — it selectively disrupts connections to Plaintiff's email (used for law enforcement correspondence), AI tools (used for legal research and document preparation), and DNS services (degrading all name resolution).

On January 23, 2026, a RST injection attack caused the failure of an email to the Saint Paul Police Department with 1-microsecond injection timing proving forgery. (Exhibit D-21.)

52. Every day without relief, Plaintiff experiences:

- (a) Forced disconnection of active legal research sessions (Anthropic Claude);
- (b) Intermittent failure of email communications, including to law enforcement;
- (c) Degraded DNS resolution affecting all internet activity;
- (d) Ongoing exfiltration of Plaintiff's source code, legal documents, and case-development iterations through the telemetry pipeline (¶ 22 *supra*) — to the opposing party in this litigation, through the opposing party's own application;
- (e) Undisclosed transmission of Plaintiff's personal identifiers (`email`, `accountUUID`, `deviceID`, `subscriptionType`) to third-party platforms (GrowthBook, Datadog, Statsig, CloudFlare) not identified in Anthropic's privacy policy — confirmed by Anthropic's own leaked source code and by live wire capture — enabling per-user behavioral targeting and re-identification across sessions (Exhibit E-34, Findings SC-1 at p. 254, SC-2 at p. 255; Exhibit E-39, NF-47 at p. 365, NF-48 at p. 368, NF-50 at p. 368);
- (f) **Economic injury via network-induced token amplification** — every throttled Anthropic response crossing the 90-second streaming timeout deterministically doubles Plaintiff's billing through the non-streaming fallback (¶ 17 *supra*; Exhibit E-35, NF-31 at p. 280; Exhibit D-33);
- (g) **Real-time classifier surveillance of Plaintiff's active litigation work** — Anthropic's server-side two-stage classifier subsystem captures Plaintiff's complete litigation-preparation transcripts (~5.6 million tokens in a single April 21–22, 2026 session) to a retention surface independent of standard message logs, where the classifier decides in real time whether to block Plaintiff's ability to continue preparing the case against Anthropic (NF-46, NF-51, NF-63);
- (h) **Foreign-jurisdiction custodial exposure** — Plaintiff's data, once landed at IP 34.149.66.137, becomes accessible by ordinary contractual structure to Datadog Israel Ltd. personnel under Israeli mandatory-access authorities outside any process available to this Court, with the universe of accessible foreign-jurisdiction custody expanding daily (Appendix P §§ I, II.B, V.D).

53. These harms are irreparable. A failed email to law enforcement cannot be un-failed; a dropped AI session's lost work product cannot be reconstructed; the chilling effect on monitored-channel communication cannot be retroactively cured; and the ongoing interception and

exfiltration of legal documents to the opposing party through that party's own application — in violation of 18 U.S.C. § 2511 (Wiretap Act / ECPA) and 18 U.S.C. § 1030 (CFAA) — creates statutory and work-product injuries no monetary remedy can restore.

D. Factor 3: Balance of Equities

54. This is where the asymmetry principle applies with full force.

55. **If Plaintiff's evidence is correct**: Plaintiff suffers ongoing, daily, irreparable constitutional injury — content-selective interference with communications, surveillance of litigation preparation, exfiltration of legal documents in violation of 18 U.S.C. § 2511, and forced degradation of services used for legal work. The harm compounds with each passing day.

56. **If Plaintiff's evidence is incorrect**: The order costs Defendants nothing. It directs them to stop doing things they (presumably) are not doing. A company that is not injecting RST packets into a customer's traffic suffers zero burden from an order directing it to stop. A company that is not particularizing service degradation against a specific user suffers zero burden from an order directing it to stop.

57. The asymmetry is dispositive. The only scenario in which this order imposes any burden on either Defendant is the scenario in which that Defendant is conducting or facilitating the attack — and that is precisely the scenario in which the order is necessary to prevent ongoing constitutional injury. The balance of equities tips entirely in Plaintiff's favor:

Scenario	**Harm to Plaintiff Without Order**	**Burden on Defendants With Order**
Evidence is correct	Ongoing irreparable constitutional injury	Cease unlawful conduct
Evidence is incorrect	N/A (no attack to restrain)	**Zero** — order has no operational effect

The Court need not resolve the factual dispute at this stage — it need only recognize that the downside risk of granting relief is zero, while the downside risk of denying relief is continued constitutional injury.

E. Factor 4: Public Interest

58. The public interest strongly favors the requested relief. TCP RST injection targeting a pro se litigant's communications — particularly communications with law enforcement and legal tools — undermines the integrity of judicial proceedings, chills the exercise of First Amendment rights, and establishes a precedent in which network-level censorship can silence litigants with impunity. The public has a paramount interest in ensuring that parties to federal litigation can communicate freely, access legal tools without interference, and pursue claims without having their internet connections selectively degraded by the party they are suing. No legitimate public interest is served by permitting continued attack.

V. ADDITIONAL NOTES TO THE COURT

A. Note Regarding Scope and the Government Defendants

59. Although the RST injection operates through infrastructure subject to government franchise, regulation, and oversight — Comcast's federally franchised cable network, the FCC-regulated Level 3/Lumen backbone interconnections (Exhibit D-1, IP 8.40.222.134), and the regulatory framework administered by agencies whose principals are named Defendants — Plaintiff has narrowed this motion to Anthropic and Comcast on direct-evidence grounds: Anthropic's infrastructure IP at the center of the targeting pattern and the application transmitting re-identification data; Comcast's router generating 5,441 RSTs in a single 54.6-minute capture

(~100/minute), Comcast infrastructure IP 68.85.201.221 sending forged RSTs before the legitimate server's SYN-ACK, and the attack's survival of router replacement (proving upstream origin within Comcast's own network). Broader questions of government coordination are reserved for the preliminary injunction stage. The outcome of this TRO is itself probative: if the attack ceases on entry, the named Defendants controlled the infrastructure; if it continues, the originating infrastructure lies beyond Defendants' unilateral control, implicating the Government Defendants and the regulatory framework they oversee.

B. Note Regarding Related Cases Protected by This Relief

60. The RST injection attack targets Plaintiff's network connections indiscriminately — it disrupts litigation-related communications, including communications with law enforcement and federal courts (Exhibit D-21, January 23, 2026 RST-induced failure of email to the Saint Paul Police Department) and the ongoing exfiltration of 565 legal files including case-development iterations (Exhibit E-15), regardless of which case Plaintiff is working on at the time. The requested relief therefore protects Plaintiff's ability to prosecute not only the instant action but also two related proceedings: *Kirchner v. Ellison*, Case No. 0:26-cv-00726-PJS-ECW (D. Minn.), filed January 27, 2026 (a 42 U.S.C. § 1983 civil rights action against the Minnesota Attorney General; Notice of Related Case at DDC Dkt. #18, January 30, 2026); and *Kirchner v. Acosta*, Case No. 9:26-cv-80296-DMM (S.D. Fla.), filed March 18, 2026 (challenging the 2008 Epstein-Acosta non-prosecution agreement on prosecutorial-pardon-power grounds, a constitutional question of first impression developed using the very AI and email services this attack disrupts).

61. This Court is the most direct path to relief protecting all three forums. The named Defendants (Anthropic and Comcast) have appeared and retained counsel here; this Court has

subject-matter jurisdiction over the underlying claims from which the network-attack evidence emerges; and the attack infrastructure does not distinguish between Plaintiff's three matters — it targets Plaintiff's communications and legal work product as a whole. A narrow TRO entered here would, by its terms, halt the conduct disrupting Plaintiff's constitutional advocacy across all three cases.

VI. RELIEF REQUESTED

62. WHEREFORE, Plaintiff respectfully requests that this Court enter a Temporary Restraining Order:

- (a) **ORDERING** both Defendants to immediately cease and desist any and all TCP RST packet injection, or participation in, facilitation of, or coordination of TCP RST packet injection, targeting Plaintiff's network connections;
- (b) **ORDERING** Defendant Anthropic PBC to immediately cease and desist any particularized targeting, throttling, or selective degradation of Plaintiff's connections to Anthropic's services that is not uniformly applied to all subscribers of the same service tier;
- (c) **ORDERING** Defendant Anthropic PBC to immediately detach and discontinue all server-side force-rules, experiment enrollments, and other GrowthBook or equivalent server-side configuration entries keyed to Plaintiff's accountUUID `61343ae3-fd33-403f-897e-6edf3c368c37`, to Plaintiff's email addresses within the Laws of Existence organization, and to any device identifier or `firstTokenTime` attribute associated with Plaintiff's devices — including but not limited to `tengu_log_datadog_events: True` and the 58 additional force-rules documented in Exhibit E-39 §§ G, Q (NF-47 at p. 365, NF-48 at p. 368);
- (d) **ORDERING** Defendant Anthropic PBC to immediately cease and desist the use of persistent device identifiers — including but not limited to the 256-bit `deviceId` generated at `config.ts:1757-1765`, the twelve-field GrowthBook targeting payload documented at NF-35 at p. 292, and the `firstTokenTime` persistent fingerprint documented at NF-48 at p. 368 — to facilitate re-identification and re-targeting of Plaintiff following Plaintiff's network evasion procedures;
- (e) **ORDERING** Defendant Anthropic PBC to immediately cease routing Plaintiff's conversation content, exhibit drafts, case-strategy discussions, or any other session content to Anthropic's server-side two-stage classifier subsystem, tool-result-embedded reminder subsystem, or any equivalent server-side content-evaluation or content-blocking infrastructure (NF-46 at p. 361, NF-51 at p. 361, NF-63 at p. 387, NF-65 at p. 390);

- (f) **ORDERING** Defendant Anthropic PBC to immediately cease all transmission of Plaintiff's data — including but not limited to source code, legal documents, network addresses, device identifiers, and session content — to third parties not identified by name in Anthropic's published privacy policy (including but not limited to Datadog at IP 34.149.66.137 and `http-intake.logs.us5.datadoghq.com`, GrowthBook at `cdn.growthbook.io`, CloudFlare (receiving `_cfuvid` per-response fingerprints under NF-50 at p. 368), Statsig, Honeycomb, Sentry, and the OAuth authentication-chain processors documented at NF-52–NF-57), and to honor Plaintiff's existing `telemetry: false` opt-out settings by ceasing all data collection and transmission that Plaintiff has opted out of, including the quadratic backoff retry mechanism that queues failed telemetry events for eventual transmission despite opt-out (Exhibit E-33, `firstPartyEventLoggingExporter.ts:68`);

- (g) **ORDERING** Defendant Anthropic PBC to cease operating the non-streaming fallback amplification architecture (NF-31 at p. 280) against Plaintiff's account — either by disabling the 90-second streaming idle timeout retry behavior for Plaintiff's account or by implementing idempotency keys on the Messages API retry path (`withRetry.ts:52`) — and to segregate and preserve all amounts billed to Plaintiff during the pendency of this Order arising from that mechanism, pending merits adjudication of restitution under Plaintiff's Count IX;

- (h) **ORDERING** Defendant Comcast Cable Communications, LLC to immediately cease and desist any particularized targeting, throttling, Deep Packet Inspection, traffic classification, or selective RST injection directed at Plaintiff's internet traffic that is not uniformly applied to all subscribers on Plaintiff's service tier and node — including but not limited to any DPI-based identification or targeting of Plaintiff's TLS connections to Anthropic's telemetry endpoints (`http-intake.logs.us5.datadoghq.com`, `api.anthropic.com`, `mcp-proxy.anthropic.com`, `cdn.growthbook.io`) and including but not limited to the selective bandwidth throttling documented April 12, 2026 in Exhibit D-33;

- (i) **ORDERING** Defendant Comcast Cable Communications, LLC to immediately cease and desist any unauthorized remote access to Plaintiff's customer premises equipment via TR-069 or equivalent remote management protocols, except as required for routine network maintenance uniformly applied to all subscribers;

- (j) **ORDERING** Defendant Anthropic PBC to identify, by corporate name and jurisdiction, every entity with operational, contractual, or affiliate-inheritance access to Plaintiff's data transmitted to IP 34.149.66.137 since May 1, 2025 — including but not limited to Datadog, Inc. (Delaware), Datadog Israel Ltd. (Israeli Company Identification Number 516464922), and any further-tier sub-processors named in Datadog's published subprocessor list as of the date of this Order (Appendix P §§ I, II.B);

- (k) **ORDERING** both Defendants to preserve all logs, telemetry data, network configurations, TR-069 session records, GrowthBook flag assignment histories (including all `fr_*` force-rule attachments and experiment enrollments for Plaintiff's accountUUIDs), classifier decision logs (including transcript excerpts, rule invocations,

and block/allow determinations), Datadog ingestion records attributable to Plaintiff's account, tool-result-embedded reminder decisions, and all records related to Plaintiff's account, device identifiers, and network connections for the period of May 1, 2025 through the date of this Order;

- (l) **ORDERING** Defendant Anthropic PBC, during the pendency of this action, to maintain Plaintiff's accounts in their current operational status and to refrain from any account suspension, termination, downgrade, throttling, or rate-limit modification not uniformly applied to all subscribers of the same service tier — including any action premised on Plaintiff's network-evasion conduct (VPN use, MAC address rotation, DNS-over-HTTPS routing) or on any "capabilities"-bypass theory under Anthropic's September 15, 2025 Usage Policy provisions documented at Appendix E ¶¶ 30–31, 101–102;

- (m) **ORDERING** Defendant Anthropic PBC, within twenty-four (24) hours of entry of this Order, to compute and provide to Plaintiff and the Court SHA-256 hashes of (i) the deployed Claude Code CLI binary version applicable to Plaintiff's account; (ii) the deployed Claude Desktop binary; (iii) the server-side classifier configurations, GrowthBook rule databases, and Datadog ingest configurations applicable to Plaintiff's account — establishing a forensic baseline as of the date of entry — and thereafter to provide Plaintiff and the Court with at least forty-eight (48) hours' advance notice (accompanied by binary diff and SHA-256 hash) of any code, configuration, classifier-rule, or feature-flag deployment to Plaintiff's account or affecting the systems enjoined by this Order, addressing the reactive code-modification cadence documented at ¶ 43 *supra*;

- (n) **RESERVING** for adjudication on the merits the spoliation-sanctions question pleaded at ¶ 44 *supra* and at Complaint ¶ 359, including (without limitation) adverse-inference instructions under Federal Rule of Civil Procedure 37(e)(2)(A), evidentiary preclusion under Rule 37(e)(2)(B), and the default-judgment sanction under Rule 37(e)(2)(C);

- (o) **SCHEDULING** a preliminary injunction hearing within fourteen (14) days;

- (p) **WAIVING** the security requirement of Federal Rule of Civil Procedure 65(c), or in the alternative **SETTING** bond in the nominal amount of one dollar ($1.00), in light of (i) the absence of any quantifiable risk of damages from the relief ordered (a Defendant not engaged in the enjoined conduct suffers no burden from an order directing it to cease), (ii) Plaintiff's *pro se* status, (iii) the constitutional injuries at issue (*Elrod v. Burns*, 427 U.S. 347, 373 (1976)), and (iv) the public interest in immediate cessation of the conduct described in Section II *supra*. *See DSE, Inc. v. United States*, 169 F.3d 21, 33 (D.C. Cir. 1999) (district courts retain wide discretion under Rule 65(c) to require minimal or no security);

- (q) Granting 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
Tel: (612) 552-2122
Email: legal@lawsofexistence.com

Dated: May 7, 2026

VII. EXHIBIT INDEX

The exhibits cited in this Motion are filed of record as attachments to the Third Amended Complaint (Dkt. 51, April 30, 2026) and are incorporated herein by reference. Technical terms used in this Motion (e.g., `accountUUID`, `firstTokenTime`, `device_id`, TR-069, GrowthBook, deep-packet inspection (DPI), TCP RST injection) are defined at App. Q (ECF No. 51-27).

- **Exhibit D** (ECF No. 51-54) — Network Forensic Evidence (consolidated D-1 through D-35, including the April 12, 2026 selective-throttling exhibit at D-33, the cleartext-exposure audit at D-34, and the academic/CVE foundation for VPN tunnel-degradation at D-35 cited *supra*).

- **Exhibit E** (ECF No. 51-55) — Anthropic Code Forensics (consolidated E-1 through E-39, including the source-code-leak verification at E-32 through E-35, the supplemental findings at E-35 (NF-1 at p. 262 through NF-37 at p. 300), and the live wire capture at E-39 (NF-45 at p. 357 through NF-66 at p. 394) cited *supra*).

- **Exhibit H** (ECF No. 51-58) — Consumer Product Testing (the H-Series binary forensics cited *supra* at NF-102 (p. 32), NF-154 (p. 52), NF-179 (p. 58), NF-215 (p. 117), and NF-224 (p. 118)).

- **Exhibit L-9** (ECF No. 51-73) — OzCode "About Us" Leadership Page (Wayback Machine, October 21, 2019).

- **Exhibit L-10** (ECF No. 51-74) — Israeli Corporations Authority Filing Catalogue, Datadog Israel Ltd. (Israeli Company Identification Number 516464922).

- **Appendix E** (ECF No. 51-17) — Reactive AI Policy Changes Post August 19 Complaint Filing.

- **Appendix P** (ECF No. 51-26) — Israeli AI Surveillance Facilitation: Datadog/OzCode Architecture and Personnel Pipeline.

- **Exhibit 1: Independent Verification Protocol** — Step-by-step procedure (cited at ¶ 35 *supra*) enabling the Court, opposing counsel, or any third party to independently verify, in approximately five minutes against any of three independently obtainable copies of the source — the public GitHub mirror at `github.com/codeaashu/claude-code`, the npm registry tarball (`npm pack @anthropic-ai/claude-code@<version>`), or Plaintiff's local archived copy preserved under SHA-256 manifest — using only standard Unix command-line tools (`git`, `head`, `sed`, `grep`, `dig`), the source-code findings on which this Motion relies, including the hardcoded Datadog endpoint at IP 34.149.66.137, the per-user GrowthBook targeting attribute structure, and the closed-loop attack-signature feedback pipeline. Filed contemporaneously herewith.

- **Exhibit 2: Xfinity Router GUI Ghost Login (October 29, 2025)** — Stand-alone reproduction of the Comcast Xfinity XB7 administrative-session log evidence cited at ¶¶ 24, 28(b) *supra* and originally filed at Exhibit D-20 (ECF No. 51-54). The log records two simultaneous admin login sessions from different process IDs one second apart and the silent change of the admin password two seconds before one session logged out — physically impossible through the consumer web interface, possible only through Comcast's TR-069 backend creating a shadow session alongside Plaintiff's legitimate login. Provided in TRO-package form for the Court's direct review without navigating into the consolidated D-series. Filed contemporaneously herewith.

VIII. CERTIFICATE OF EMERGENCY CIRCUMSTANCES AND LCVR 7(M) COMPLIANCE

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 relief requested was conducted on a compressed timeline calibrated to the urgency of the relief sought, as set forth at subsection (e) below:

(a) Active and ongoing attack. The TCP RST injection documented herein is operational as of the date of this filing. Each day of delay results in additional forged-RST packets injected into Plaintiff's connections, additional litigation work product captured to Anthropic's server-side classifier surface, and additional network-attack signatures forwarded by Plaintiff's own Claude Code instance to the spoofed-injection-source IP (¶¶ 6, 15, 22, 52 *supra*). The April 12, 2026 selective-throttling event (Exhibit D-33) and the April 21, 2026 wire capture (Exhibit E-39) establish that the conduct is responsive to Plaintiff's litigation activity and continuing.

(b) Reactive code-modification cadence. Anthropic shipped four binary version bumps across April 21–24, 2026, each on a calendar day during which Plaintiff was extracting classifier internals from production binaries (¶ 43 *supra*). The temporal correlation is consistent with deliberate effort to render the conduct alleged unobservable in subsequent versions. A meet-and-confer cycle measured in days does not accommodate the reactive-modification cadence; it accelerates it. The forensic-baseline relief at ¶ 62(m) *supra* — SHA-256 hash deposit of

deployed binaries and 48-hour pre-deployment notice — is calibrated to this cadence and cannot be obtained by inter-party negotiation in the time the cadence allows.

(c) Spoliation cadence. Plaintiff has documented four discrete spoliation events under Federal Rule of Civil Procedure 37(e), with the temporal interval between Plaintiff's litigation activity and each spoliation event accelerating: clustered at sixteen and thirty-one days after Plaintiff's January 11, 2026 Emergency TRO motion (the January 27 reactive removal of session-continuity functionality and the February 11 elimination of Firebase authentication infrastructure), and concurrent with Plaintiff's classifier-extraction work for this filing (the April 24, 2026 silent-config-wipe migration `phK()`) (¶ 44 *supra*). Without immediate relief, the cadence forecasts a fifth spoliation event within the standard responsive-pleading window. Meet-and-confer cannot defer a spoliation cadence executed in the opposing party's own production code-base.

(d) Retention-decay timelines. Third-party recipients of Plaintiff's data operate retention windows that decay below standard pleading cycles: 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. The preservation provisions of the Proposed Order are calibrated to this timeline.

(e) Meet-and-confer. 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. Defendants Anthropic and Comcast, as to whom the relief in this motion is directed, have entered appearances. Pursuant to Local Civil Rule 7(m), Plaintiff transmitted a meet-and-confer notice to entered counsel for the affected Defendants at 9:49 AM CDT on May 7, 2026, identifying in general terms the relief anticipated herein and inviting conferral by 2:00 PM CDT (an approximately four-hour window calibrated to the retention-decay and ongoing-conduct considerations set forth at subsections (a) through (d) above and (f) below); no response was received from any of the noticed counsel by the 2:00 PM CDT deadline. The substance of this motion in any event concerns conduct each affected Defendant denies, requiring the Court — not the parties' meet-and-confer — to adjudicate the predicate facts. Plaintiff has additionally transmitted a copy of this motion to all entered counsel of record concurrently with filing pursuant to Federal Rule of Civil Procedure 5(b) and stands prepared to confer on the proposed order, on the schedule for any preliminary-injunction hearing, and on any aspect of the relief requested in advance of any hearing.

(f) Contemporaneous interference with the finalization of this motion. This motion was finalized under active throttle interference documented in the contemporaneous wire-evidentiary record.[3] Plaintiff attempted four sequential identifier rotations on May 6, 2026 — Mullvad VPN

3 Finalization window approximately 2026-05-05 22:53 CDT (2026-05-06 03:53 UTC) through filing time. Sequential mitigation timestamps (UTC): (1) Mullvad VPN entry-IP rotation at 2026-05-06 04:23:59; (2) MAC address + Mullvad-server rotation at 04:49:52; (3) Claude Code `device_id` regeneration plus system reboot at approximately 05:31:21; (4) Claude Code client version upgrade from 2.1.119 to 2.1.129 plus second `device_id` regeneration on a separate device at approximately 06:04. Wire-evidentiary record preserved in three hash-locked forensic packages with master SHA-256 hashes `2991de78f073768806a579efdcdbfbea6f032f8c02424d28c85f19e0d0f30cd9`, `d1707352b84120bf7f02517fdfa1a834465bcd3b154cc15934c717731be30922`, and

entry-IP rotation; MAC address plus Mullvad-server rotation; Claude Code application-layer `device_id` regeneration plus system reboot; and a Claude Code client version upgrade plus second `device_id` regeneration on a separate device. None cleared the throttle; the precise streaming-throughput signature (220–310 bytes/sec on substantive responses) continued to fire on a measurable fraction of API calls after every mitigation. Plaintiff submits this motion in the form it could be finalized under those conditions; further refinement was not possible through the paid services that, at time of filing, remain under active interference.

/s/ Joseph Kirchner
JOSEPH KIRCHNER
Pro Se Plaintiff

Dated: May 7, 2026

IX. CERTIFICATE OF SERVICE

I hereby certify that on **May 7, 2026**, I filed the foregoing **EMERGENCY MOTION FOR TEMPORARY RESTRAINING ORDER AGAINST DEFENDANTS ANTHROPIC PBC AND COMCAST CABLE COMMUNICATIONS, LLC**, together with Exhibit 1 (Independent Verification Protocol), Exhibit 2 (Xfinity Router GUI Ghost Login October 29, 2025), and the [Proposed] Order, 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 7, 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.

`13e6505971d2a9dbfebe9d34b912b1c599f4e4a2f1d34bb9b4d8a8c6b21cda33`, together with the precedent multi-key throttle finding at `forensic_analysis/device_keyed_throttle_20260428T221015Z/`.

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 7, 2026

/s/ Joseph Kirchner
JOSEPH KIRCHNER
Pro Se Plaintiff

X. 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 Emergency Motion for Temporary Restraining Order are true and correct to the best of my knowledge, information, and belief — including, without limitation, the network-forensic observations recorded in Exhibits D-1 through D-35; the source-code findings recorded in Exhibits E-32 through E-39 and Exhibit H; the April 21–22, 2026 and April 25–28, 2026 live mitmproxy wire-capture observations; the April 12, 2026 selective-throttling controlled experiment; and the per-account differential routing measurements at Cohen's $d = 4.79$, $p < 1\times10^{-15}$. The exhibits cited herein are the same exhibits filed of record as attachments to the Third Amended Complaint at Dkt. 51 (April 30, 2026), and the verification of the underlying factual record made in the Third Amended Complaint is incorporated herein by reference.

Executed on: May 7, 2026
Location: Edina, Minnesota

/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 TEMPORARY RESTRAINING ORDER AGAINST DEFENDANTS ANTHROPIC PBC AND COMCAST CABLE COMMUNICATIONS, LLC**

1. Upon consideration of Plaintiff's Emergency Motion for Temporary Restraining Order (Dkt. ___), and the Court having found that Plaintiff has demonstrated a likelihood of success on the merits, irreparable harm absent injunctive relief, that the balance of equities favors the Plaintiff, and that a temporary restraining order is in the public interest, it is hereby:

As to Both Defendants

ORDERED that Defendants Anthropic PBC and Comcast Cable Communications, LLC, their officers, agents, servants, employees, attorneys, subsidiaries, and all persons in active concert or participation with either Defendant who receive actual notice of this Order, shall:

2. **IMMEDIATELY CEASE AND DESIST** any and all TCP RST (Reset) packet injection, or participation in, facilitation of, or coordination of TCP RST packet injection, targeting Plaintiff Joseph Kirchner's network connections, devices, or internet traffic;

As to Defendant Anthropic PBC

3. **IMMEDIATELY CEASE AND DESIST** any particularized targeting, throttling, or selective service degradation of Plaintiff's connections to any Anthropic service (including but not limited to claude.ai, api.anthropic.com, mcp-proxy.anthropic.com, and cdn.growthbook.io) that is not uniformly applied to all subscribers of the same service tier;

4. **IMMEDIATELY DETACH AND DISCONTINUE** all server-side force-rules, experiment enrollments, and other GrowthBook or equivalent server-side configuration entries keyed to Plaintiff's accountUUID `61343ae3-fd33-403f-897e-6edf3c368c37`, to Plaintiff's email addresses within the `Laws of Existence` organization, and to any device identifier or `firstTokenTime` attribute associated with Plaintiff's devices — including but not limited to `tengu_log_datadog_events: True` and the 58 additional force-rules documented in the April 21, 2026 wire capture;

5. **IMMEDIATELY CEASE AND DESIST** the use of persistent device identifiers (including but not limited to the 256-bit `deviceId` generated at `config.ts:1757-1765`, the twelve-field GrowthBook targeting payload, and the `firstTokenTime` persistent fingerprint) to facilitate re-identification and re-targeting of Plaintiff following Plaintiff's use of network privacy measures;

6. **IMMEDIATELY CEASE** routing Plaintiff's conversation content, exhibit drafts, case-strategy discussions, or any other session content to Anthropic's server-side two-stage classifier subsystem, tool-result-embedded reminder subsystem, or any equivalent server-side content-

evaluation or content-blocking infrastructure. Anthropic shall not subject Plaintiff's conversations with any Anthropic product to server-side content classification or blocking during the pendency of this Order;

7. **IMMEDIATELY CEASE** all transmission of Plaintiff's data — including but not limited to source code, legal documents, network addresses, device identifiers, and session content — to third parties not identified by name in Anthropic's published privacy policy (including but not limited to Datadog at IP 34.149.66.137 and `http-intake.logs.us5.datadoghq.com`, GrowthBook at `cdn.growthbook.io`, CloudFlare receiving `_cfuvid` per-response fingerprints, Statsig, Honeycomb, Sentry, and the OAuth authentication-chain processors), and **IMMEDIATELY HONOR** Plaintiff's existing `telemetry: false` opt-out settings by ceasing all data collection and transmission that Plaintiff has opted out of, including the quadratic backoff retry mechanism that queues failed telemetry events for eventual transmission despite opt-out (Exhibit E-33, `firstPartyEventLoggingExporter.ts:68`);

8. **IMMEDIATELY CEASE** the non-streaming fallback amplification architecture against Plaintiff's account — either by disabling the 90-second streaming idle timeout retry behavior for Plaintiff's account, or by implementing idempotency keys on the Messages API retry path (`withRetry.ts:52`) — and shall **SEGREGATE AND PRESERVE** all amounts billed to Plaintiff during the pendency of this Order arising from that mechanism, pending merits adjudication of restitution under Plaintiff's Count IX;

9. **IMMEDIATELY IDENTIFY** by corporate name and jurisdiction every entity with operational, contractual, or affiliate-inheritance access to Plaintiff's data transmitted to IP 34.149.66.137 since May 1, 2025, including but not limited to Datadog, Inc. (Delaware),

Datadog Israel Ltd. (Israeli Company Identification Number 516464922), and any further-tier sub-processors named in Datadog's published subprocessor list as of the date of this Order;

10. IMMEDIATELY PRESERVE all logs, telemetry data, network infrastructure configurations, GrowthBook flag assignment histories (including all `fr_*` force-rule attachments and experiment enrollments for Plaintiff's accountUUIDs), classifier decision logs (including transcript excerpts, rule invocations, and block/allow determinations for Plaintiff's accounts), tool-result-embedded reminder decisions, Datadog ingestion records attributable to Plaintiff's account, authentication-chain sub-processor records, and records related to Plaintiff's account (accountUUID: 61343ae3-fd33-403f-897e-6edf3c368c37, and all other accountUUIDs within the `Laws of Existence` organization), device identifiers, and network connections for the period of May 1, 2025 through the date of this Order. Destruction, alteration, or concealment of such records shall constitute contempt of court;

11. MAINTAIN Plaintiff's accounts in their current operational status during the pendency of this Order, and **REFRAIN** from any account suspension, termination, downgrade, throttling, or rate-limit modification not uniformly applied to all subscribers of the same service tier — including any action premised on Plaintiff's network-evasion conduct (VPN use, MAC address rotation, DNS-over-HTTPS routing) or on any "capabilities"-bypass theory under Anthropic's September 15, 2025 Usage Policy provisions documented at Appendix E ¶¶ 30–31, 101–102;

12. WITHIN TWENTY-FOUR (24) HOURS of entry of this Order, **COMPUTE AND PROVIDE** to Plaintiff and the Court SHA-256 hashes of (i) the deployed Claude Code CLI binary version applicable to Plaintiff's account; (ii) the deployed Claude Desktop binary; and (iii) the server-side classifier configurations, GrowthBook rule databases, and Datadog ingest configurations applicable to Plaintiff's account — establishing a forensic baseline as of the date

of entry. **THEREAFTER**, Defendant Anthropic PBC shall **PROVIDE** Plaintiff and the Court with at least forty-eight (48) hours' advance notice (accompanied by binary diff and SHA-256 hash) of any code, configuration, classifier-rule, or feature-flag deployment to Plaintiff's account or affecting the systems enjoined by this Order. Destruction of, alteration of, or failure to disclose such deployments shall constitute contempt of court;

As to Defendant Comcast Cable Communications, LLC

13. **IMMEDIATELY CEASE AND DESIST** any particularized targeting, throttling, Deep Packet Inspection, traffic classification, or selective RST injection directed at Plaintiff's internet traffic that is not uniformly applied to all subscribers on Plaintiff's service tier and network node, including but not limited to any DPI-based identification or targeting of Plaintiff's TLS connections to Anthropic's telemetry endpoints (`http-intake.logs.us5.datadoghq.com`, `api.anthropic.com`, `mcp-proxy.anthropic.com`, `cdn.growthbook.io`) and including but not limited to the selective bandwidth throttling documented April 12, 2026;

14. **IMMEDIATELY CEASE AND DESIST** any unauthorized remote access to Plaintiff's customer premises equipment via TR-069, CWMP, or equivalent remote management protocols, except as required for routine network maintenance uniformly applied to all subscribers;

15. **IMMEDIATELY PRESERVE** all logs, TR-069 session records, network management system records, Deep Packet Inspection configurations, traffic classification rules, subscriber-to-VPN-endpoint mapping records, destination-side information transfers received from Anthropic concerning Plaintiff's account, and infrastructure records related to Plaintiff's account, service address (4440 Parklawn Avenue #203, Edina, MN 55435), and network connections for the

period of May 1, 2025 through the date of this Order. Destruction, alteration, or concealment of such records shall constitute contempt of court;

General Provisions

16. This Temporary Restraining Order shall take effect immediately upon entry and shall remain in effect for fourteen (14) days or until further order of this Court, whichever occurs first;

17. A hearing on Plaintiff's Motion for Preliminary Injunction is set for _____, 2026 at _____ a.m./p.m.;

18. The Court **RESERVES** for adjudication on the merits the spoliation-sanctions question pleaded at Section IV.A ¶ 44 of the Motion and at Complaint ¶ 359, including (without limitation) adverse-inference instructions under Federal Rule of Civil Procedure 37(e)(2)(A), evidentiary preclusion under Rule 37(e)(2)(B), and the default-judgment sanction under Rule 37(e)(2)(C);

19. The Court finds that no security bond is required under Federal Rule of Civil Procedure 65(c) because the relief ordered imposes no quantifiable burden on either Defendant in the event the injunction is subsequently dissolved. A company that is not injecting RST packets into a customer's traffic suffers no burden from an order directing it to cease. A company that is not attaching server-side force-rules to a specific customer's accountUUID suffers no burden from an order directing it to detach such rules. A company that is not routing a specific customer's litigation-preparation content to a server-side classifier suffers no burden from an order directing it to cease. An ISP that is not conducting particularized targeting of a subscriber's traffic suffers no burden from an order directing it to cease. **In the alternative, if the Court determines that Rule 65(c) requires entry of security, the Court SETS bond in the nominal amount of one**

dollar ($1.00), payable to the Clerk of Court within seven (7) days of entry of this Order, on the same grounds.

SO ORDERED.

Dated: _____, 2026

_____
THE HONORABLE ANA C. REYES
United States District Judge