UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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

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

DISCOVERY-7: DEFENDANT COMCAST CABLE COMMUNICATIONS, LLC (AND RELATED NETWORK-TIER CUSTODIANS)

INTRODUCTION

Discovery-7 separates the ISP, backbone, and attack-platform custodians from DISCOVERY-4's government defendants because the evidentiary predicate has changed materially since the January 2026 draft:

1. **Anthropic's March 31, 2026 source code release** (Ex. E-32 at p. 235, l. 3) independently verifies that the Datadog telemetry endpoint `34.149.66.137` is hardcoded at `datadog.ts:12-14` of Claude Code CLI (Ex. E-34, Finding SC-9). The same IP appears as the claimed source of **327 spoofed RST packets** on March 12, 2026 in the network forensic record

(Ex. D-26 at p. 137, l. 17), establishing a concrete cross-layer bridge between source-code telemetry infrastructure and alleged ISP-level packet injection.

2. **D-series network forensic exhibits (D-1 through D-33, D-35)** now document 260,395+ TCP RST packets, a tool fingerprint (80-83% bare-RST ratio; 92-98% under hardware TAP conditions), microsecond-precision burst automation proving non-human origin, and the smoking-gun identification of a VMware attack platform with MAC `00:0c:29:50:89:f1` (Ex. D-3 at p. 13, l. 29).

3. **NF-31 (Network-Induced Token Amplification)** documents an architecturally-guaranteed 2× billing cascade when ISP throttling (Ex. D-33 at p. 200, l. 7) pushes Anthropic API streaming past its 90-second idle timeout (Ex. E-35, Finding NF-31). This ties Comcast's network behavior directly to Plaintiff's financial injury under Counts IX, X, and XII.

Each request below identifies its evidentiary predicate and the legal counts it develops. The Pleading Pipeline's citation grammar is used throughout; exhibit and finding citations auto-resolve against the current filing index so the rendered document always reflects the correct exhibit numbers and page references.

DEFINITIONS AND CONVENTIONS

For purposes of this discovery document, the following terms have the meanings given:

- **"Plaintiff's IP range"** means any IPv4 or IPv6 address assigned by Comcast to Plaintiff's residential service (the account associated with Comcast Xfinity Router Serial `21V4H5FHDA00031`) during the period October 1, 2024 through the date of production, including CGNAT-assigned addresses within `68.80.0.0/13` (JUMPSTART-2) and any successor allocation block.

- **"Anthropic-bound traffic"** means any network flow whose destination IP resolves (or at the time of capture resolved) to any of `api.anthropic.com`, `statsig.anthropic.com`, or any IP of record published by Anthropic PBC in its source code as a telemetry or API endpoint, including but not limited to `34.149.66.137` (Datadog) as hardcoded at `datadog.ts:12-14`.

- **"Bare RST"** means a TCP segment with only the RST flag set (TCP flags byte `0x04`), no payload, and no accompanying ACK.
- **"Microsecond burst"** means two or more TCP RST segments separated by an inter-arrival interval of less than 100 microseconds.
- **"Spoofed RST"** means a TCP RST segment whose claimed source IP, when analyzed for TTL, MSS, window-scale, or TCP timestamp signature, is inconsistent with the network distance or stack fingerprint of the claimed origin.

Relevant period, unless otherwise specified: **October 1, 2024 through the date of production.**

Production format: Native-format packet captures (`.pcap` / `.pcapng`), router logs in their native binary or structured text form, and TR-069 ACS backend records in their native database or log-file form. Redaction for unrelated customer data is permitted pursuant to a mutually negotiated protective order; redactions must be accompanied by a redaction log identifying the nature and legal basis of each redaction.

TOPIC ALIASES (FOR CROSS-REFERENCE FROM PLAINTIFF'S MOTIONS)

The Renewed Emergency Motion for Expedited Discovery and Immediate Preservation Order references the topic-keyed sections within this document. The following table maps those references to the corresponding Phase / Category labels:

Motion reference	This document
§ Selective-Throttling-Architecture	Phase 5 (NF-31 × D-33 Token Amplification); cross-referenced at Phase 1 Category A and Phase 2

PHASE 1: CROSS-LAYER DEFENDANT COORDINATION (21 DAYS)

CATEGORY A: DATADOG ENDPOINT (34.149.66.137) TRAFFIC AND COORDINATION

REQUEST NO. 1: All netflow, packet-capture, or DPI records showing traffic between any Comcast-operated network segment and IP `34.149.66.137` during the relevant period, including:

(a) Complete 5-tuple flow records (src IP, dst IP, src port, dst port, protocol)

(b) Packet counts, byte counts, and TCP flag distributions (SYN / ACK / FIN / RST)

(c) Temporal correlation logs for any flow whose source IP is `34.149.66.137`

(d) TTL values for all packets claiming `34.149.66.137` as source IP

(e) Any internal notations, tickets, or annotations referencing this IP

Evidentiary predicate: This IP is hardcoded at `datadog.ts:12-14` in Anthropic's Claude Code CLI source code as the Datadog telemetry endpoint (Ex. E-34, Finding SC-9). The same IP appears as the claimed source of **327 spoofed RST packets** targeting Plaintiff on March 12, 2026 (Ex. D-26 at p. 137, l. 17). High-TTL analysis (TTL 240-249) proves source-IP spoofing for packets claiming this origin (Ex. D-27 at p. 141, l. 29). **Counts developed:** Compl., Count XII (ECPA, 18 U.S.C. § 2511), Compl., Count XIII (CFAA, 18 U.S.C. § 1030), Compl., Count V (42 U.S.C. § 1985 Conspiracy).

REQUEST NO. 2: All logs, alerts, or investigations generated by Comcast's deep-packet-inspection, anomaly-detection, or netflow-analysis systems regarding:

(a) Volume anomalies in traffic purportedly originating from `34.149.66.137`

(b) TTL irregularities for packets claiming Google Cloud Platform origination

(c) Cross-correlation between legitimate Datadog telemetry patterns and anomalous RST bursts claiming the same source IP

Evidentiary predicate: The mathematical proof of packet forgery (Ex. D-24 at p. 129, l. 19) establishes that 327 packets claiming `34.149.66.137` origination cannot have traversed the measured path without manipulation at a Comcast-controlled hop.

REQUEST NO. 3: All communications, contracts, peering agreements, or mutual-assistance arrangements between Comcast and any of: (a) Anthropic PBC; (b) Google LLC or Google Cloud Platform; (c) Datadog, Inc.; (d) any intermediary contracting on behalf of those entities, relating to:

(a) Traffic marking, prioritization, or interception of Anthropic-bound or Datadog-bound flows

(b) Lawful-intercept capabilities terminating at Google Cloud addresses

(c) Any cooperative arrangement permitting one party to inject, spoof, or appear as the other on Comcast's network

Evidentiary predicate: The cross-layer bridge established by Ex. D-31 at p. 170, l. 3 cannot be explained by arms-length ISP operation. Supports Compl., Count V (42 U.S.C. § 1985 Conspiracy) and Compl., Count VI (RICO, 18 U.S.C. § 1962).

REQUEST NO. 4: All documentation of Comcast's policies and technical implementations for handling packets whose claimed source IP is a large cloud provider's address space (GCP `34.0.0.0/8`, AWS `3.0.0.0/8` and `52.0.0.0/8`, Azure `20.0.0.0/8`), including:

(a) Source-address validation (BCP 38 / RFC 2827) deployment maps

(b) Whether spoof-prevention is enforced at peering, edge, or customer boundaries

(c) Any exceptions, waivers, or disabling of spoof prevention for specific peering relationships, customers, or government requestors

Evidentiary predicate: The existence of 327 spoofed packets claiming GCP origination reaching Plaintiff's network establishes either (a) Comcast does not enforce source-address validation on this peering edge, or (b) the spoofing originates inside Comcast's own network. Either finding supports Compl., Count XIII (CFAA, 18 U.S.C. § 1030).

REQUEST NO. 5: All communications, policy memoranda, or operational guidance regarding Comcast's handling of litigation-reference traffic where the cross-defendant parties include both a Comcast customer (Plaintiff) and a non-Comcast cloud-hosted entity (Anthropic PBC), including:

(a) Policies requiring isolation, preservation, or special handling of such flows

(b) Legal-hold instructions issued to network operations staff

(c) Any deviation from standard operational procedures observed in Plaintiff's IP range

Evidentiary predicate: Supports preservation obligation under Federal Rule of Civil Procedure 37(e).

PHASE 2: BACKBONE AND LAST-MILE RST INJECTION (21 DAYS)

CATEGORY B: LEVEL 3 / LUMEN TECHNOLOGIES BACKBONE (IP 8.40.222.134)

Note: These requests are directed to Comcast in its capacity as a peering counterparty of Level 3 / Lumen Technologies and as custodian of netflow data crossing that peering boundary. Parallel requests are directed to Level 3 / Lumen Technologies as a DOE defendant upon service.

REQUEST NO. 6: All netflow, packet-capture, or interconnection logs at Comcast's peering boundary with Level 3 / Lumen Technologies for traffic involving IP `8.40.222.134` and Plaintiff's IP range during the relevant period, including:

(a) Direction of traffic (toward or away from Plaintiff)
(b) TCP flag distributions, with particular attention to RST-only flows
(c) Inter-arrival timing for all RST segments crossing this boundary
(d) TTL values at the point of ingress to Comcast's network

Evidentiary predicate: Ex. D-1 at p. 3, l. 1 documents RST injection at the Level 3 / Lumen backbone identified by IP `8.40.222.134`. Ex. D-22 at p. 121, l. 11 demonstrates victim-specific targeting at the backbone tier.

REQUEST NO. 7: All peering agreements, interconnection contracts, and operational memoranda between Comcast and Level 3 / Lumen Technologies governing:

(a) Traffic-shaping, QoS, or filtering applied at the peering boundary
(b) Any mutual-aid provisions for lawful-intercept, anti-DDoS, or content-filtering operations
(c) Any arrangement under which one carrier may inject, drop, or modify traffic on the other's behalf

Evidentiary predicate: Supports Compl., Count XII (ECPA, 18 U.S.C. § 2511) by establishing whether the injection path is contractually sanctioned.

REQUEST NO. 8: All communications between Comcast and Level 3 / Lumen Technologies regarding Plaintiff, Plaintiff's IP range, or any traffic destined to Anthropic PBC, Apple, Inc., or OpenAI, Inc. infrastructure during the relevant period.

REQUEST NO. 9: All documents sufficient to identify the complete AS-level path and physical interconnection facility through which traffic between Plaintiff and each of `api.anthropic.com`, `api.openai.com`, and Apple's Floodgate proxy infrastructure (Ex. F-4 at p. 22, l. 2) traversed during the relevant period, including:

(a) BGP routing tables at representative timestamps
(b) Physical interconnection facility identifications (co-location addresses)
(c) Fiber path documentation
(d) Any alternate paths available but not used

Evidentiary predicate: Ex. D-30 at p. 160, l. 7 establishes the "every hop between modem and internet is Comcast-owned" finding; this request develops the record on the specific facilities involved.

REQUEST NO. 10: All operational tickets, incident reports, or maintenance windows affecting the Comcast-Level 3 / Lumen peering boundary on the following high-volume attack days documented in Plaintiff's network forensic record:

(a) January 6, 2026 (1,680 RST events) — Ex. D-16 at p. 72, l. 29

(b) January 7-8, 2026 (11,773 events over 13 hours) — Ex. E-24 at p. 159, l. 2

(c) January 9, 2026 (28,561 RSTs, peak single day) — Ex. D-7 at p. 38, l. 11

(d) February 25, 2026 (50,516 RSTs, all-time peak) — Ex. D-25 at p. 134, l. 16

(e) March 12, 2026 (27,238 RSTs, multi-vector) — Ex. D-26 at p. 137, l. 17

(f) March 17-22, 2026 (sustained campaign) — Ex. D-28 at p. 147, l. 9

CATEGORY C: COMCAST JUMPSTART-2 NETWORK AND INJECTION POINT 68.85.201.221

REQUEST NO. 11: Complete technical and operational documentation of Comcast's JUMPSTART-2 network (`68.80.0.0/13`), including:

(a) Network architecture diagrams

(b) Equipment inventory at the identified injection point `68.85.201.221`

(c) Capabilities of equipment at that point to originate, modify, or inject TCP segments

(d) Deployment date and authorizing documentation for any packet-injection capability

(e) Access control, audit logging, and monitoring for that equipment

Evidentiary predicate: Ex. D-12 at p. 52, l. 28 identifies this network and IP as the specific injection locus; Ex. D-29 at p. 153, l. 32 documents the tool signature.

REQUEST NO. 12: All logs from equipment at the JUMPSTART-2 injection point (`68.85.201.221`) for the relevant period, including:

(a) Administrative session logs (who connected, when, from where, for what duration)

(b) Configuration-change logs with timestamps and authorization chains

(c) Packet-injection or packet-modification logs, if any such logging exists

(d) Any logs showing commands to originate packets claiming source IPs other than the equipment's own address

REQUEST NO. 13: All documents regarding the relationship between Comcast's CGNAT infrastructure (RFC 1918 internal addressing) and JUMPSTART-2's customer-facing addressing, specifically the translation boundary through which Plaintiff's traffic traverses, including:

(a) Logs of CGNAT sessions associated with Plaintiff's account

(b) Documentation of whether CGNAT translation preserves or modifies TCP flag fields

(c) Any traffic-shaping or filtering applied at the CGNAT boundary

REQUEST NO. 14: All communications and policy documents regarding:

(a) Selective throttling or deep-packet-inspection applied to specific destinations within Plaintiff's IP range

(b) Any "slow-lane" or degraded-service policy targeting AI-platform traffic

(c) The operational basis for the selective throttling finding in Ex. D-33 at p. 200, l. 7

Evidentiary predicate: Ex. D-33 at p. 200, l. 7 documents ISP bandwidth throttling paired with NF-31's source code mechanism; this request develops the record on the ISP side of that pair.

REQUEST NO. 15: All documents regarding Comcast's Public IP `66.41.6.122` and its relationship to the relevant period, including:

(a) Whether this IP was ever assigned to Plaintiff's service

(b) Any injection, monitoring, or DPI activity associated with this IP

(c) Internal references to this IP in attack-related or customer-complaint tickets

Evidentiary predicate: Ex. D-1 at p. 3, l. 1 identifies `66.41.6.122` as the Comcast victim IP during the backbone-injection attack.

REQUEST NO. 16: All records of VPN detection or anti-VPN countermeasures deployed against Plaintiff's service, including:

(a) Traffic-pattern analysis identifying VPN usage

(b) Selective degradation or filtering of VPN traffic

(c) Any response to Plaintiff's VPN use documented in Ex. D-2 at p. 6, l. 12 (614 → 0 RSTs) and Ex. D-34 at p. 217, l. 18

CATEGORY D: ATTACK PATTERN FINGERPRINTING

REQUEST NO. 17: All documentation, specifications, source code, firmware, or operational records regarding equipment on Comcast's network capable of emitting **TCP RST segments with only the RST flag set (bare RST, flags byte `0x04`), no payload, and no accompanying ACK**, including:

(a) Vendor, make, model, and firmware version of any such equipment

(b) Deployment locations and dates

(c) Access-control and audit logging for each deployment

(d) Any documentation of the operational purpose of bare-RST emission

Evidentiary predicate: Ex. D-29 at p. 153, l. 32 documents an 80-83% bare-RST ratio as a tool fingerprint isolating a single injection instrument; Ex. D-32 at p. 192, l. 19 documents a 92-98% bare-RST

ratio under hardware-TAP conditions. Commercial TCP stacks do not emit bare RSTs in this proportion during normal operation.

REQUEST NO. 18: All documentation regarding equipment capable of emitting multiple TCP RST segments at sub-100-microsecond inter-arrival intervals ("microsecond bursts") on Comcast's network, including:

(a) Hardware capable of such timing precision (commercial software TCP stacks cannot)
(b) Deployment locations and authorization records
(c) Any legitimate operational purpose for such bursts

Evidentiary predicate: Ex. D-24 at p. 129, l. 19 documents 1-microsecond FIN-to-RST gaps establishing physical impossibility of software-only origination; Ex. D-29 at p. 153, l. 32 documents triplicate-burst patterns (three RSTs at sequence numbers X, X, X+1 within 1-2 microseconds) consistent with a dedicated injection appliance.

REQUEST NO. 19: All deployment, authorization, and operational records for hardware-TAP or wire-tap infrastructure anywhere in the path between Plaintiff's residential service and Comcast's peering boundaries, including:

(a) Physical TAP equipment (passive or active)
(b) Authorization records (court order, NSL, FISA, administrative, or operational)
(c) Audit logs of TAP activation periods
(d) Identification of any TAP-adjacent injection capability

Evidentiary predicate: Ex. D-32 at p. 192, l. 19 documents a 92-98% bare-RST ratio observed during April 2026, consistent with wire-level injection at TAP-adjacent equipment.

REQUEST NO. 20: All logs of RST-flood, DDoS, or anomaly-detection alerts that should have been triggered by the following documented RST volumes targeting Plaintiff's IP range:

(a) 28,561 RSTs on January 9, 2026 (single-day peak)
(b) 50,516 RSTs on February 25, 2026 (all-time peak)
(c) 11,773 events over 13 hours, January 7-8, 2026
(d) Sustained 6-day, 75,000-RST campaign documented in Ex. D-28 at p. 147, l. 9

For each event, produce: (a) the alert record if one was generated; (b) the resolution notes; (c) if no alert was generated, documentation of the thresholds and why they were not exceeded.

Evidentiary predicate: Absence of alerts at these volumes is itself probative of either (a) Comcast's monitoring was disabled for Plaintiff's IP range, or (b) Comcast originated or sanctioned the traffic.

REQUEST NO. 21: All records showing packet-capture or netflow data for Plaintiff's IP range during the 24-hour period bracketing each of the attack events listed in REQUEST NO. 20, sufficient to establish:

(a) Whether RST volumes matched those recorded in Plaintiff's forensic captures
(b) Whether Comcast-side captures show any traffic Plaintiff's client-side captures do not (or vice versa)
(c) The direction of RST segments relative to the peering boundary

PHASE 3: TR-069 / ROUTER FORENSICS (IMMEDIATE — PRESERVATION CRITICAL)

CATEGORY E: TR-069 ACS BACKEND LOGS

REQUEST NO. 22: All TR-069 Auto Configuration Server (ACS) backend logs for router Serial `21V4H5FHDA00031`, and for any predecessor or successor equipment on Plaintiff's account, during the relevant period, including:

(a) Complete administrative command history pushed to the device
(b) Session logs showing connection time, duration, source IP, and authentication credentials for every administrative session
(c) Configuration changes with before/after snapshots
(d) Firmware update events
(e) Any session whose duration is anomalous (less than 5 seconds or exceeding normal maintenance windows)
(f) Session termination logs and reasons

Evidentiary predicate: Ex. D-20 at p. 107, l. 28 documents the pattern; Ex. D-15 at p. 65, l. 13 documents router-side RST originating from the device.

REQUEST NO. 23: All documentation regarding the October 29, 2025 one-second administrative session on router Serial `21V4H5FHDA00031`, including:

(a) Technical explanation of session purpose
(b) Authorization records
(c) Identity of the personnel or automated system that initiated the session
(d) Commands executed during the session
(e) Why the session terminated at exactly one second
(f) Whether this pattern represents standard operational procedure or an anomaly

REQUEST NO. 24: Complete technical documentation of the TR-069 ACS system's capabilities, including:

(a) Real-time user-activity monitoring architecture
(b) Automated response mechanisms with sub-second deployment capability
(c) Government-access interfaces and integration points
(d) Law enforcement coordination systems (LESRC integration)
(e) Audit logging of automated ACS actions
(f) Deployment dates for each surveillance-capable feature

REQUEST NO. 25: All documentation regarding automated systems that detect a customer's administrative login to their own router and trigger automated shadow sessions or configuration pushes, including:

(a) System configurations for automated detection
(b) Trigger rules creating automated administrative sessions
(c) Alert systems monitoring user router access
(d) Automated response protocols executed on October 29, 2025, between 19:50:54 and 19:50:55
(e) Backend monitoring architecture enabling one-second response capability

CATEGORY F: ROUTER FIRMWARE (TG1682G, XB7, XB8)

REQUEST NO. 26: All firmware versions, modifications, and source code for the following Comcast customer-premises equipment deployed during the relevant period:

(a) Arris TG1682G (Comcast Xfinity Router, as deployed to Plaintiff)
(b) Arris TG4482 (Comcast XB7 Router)
(c) Technicolor CGM4981COM (Comcast XB8 Router)

Production shall include: (a) baseline firmware images for each model; (b) any account-specific or serial-specific firmware modifications; (c) any firmware modifications enabling real-

time user-activity reporting to backend systems; (d) any firmware enabling packet-origination (RST or other TCP segments) from the CPE.

Evidentiary predicate: Ex. D-19 at p. 85, l. 31 documents the security architecture of XB7/XB8; Ex. D-15 at p. 65, l. 13 documents RST origination from CPE.

REQUEST NO. 27: All firmware update logs for Serial `21V4H5FHDA00031` during the relevant period, including:

(a) Deployment timestamps
(b) Version before and after each update
(c) Authorization chain for each update
(d) Comparison to standard firmware release schedule for the device model
(e) Any updates initiated outside the standard release schedule

REQUEST NO. 28: All documentation of capabilities in Comcast CPE firmware for kernel-level connection filtering on hosts connected to the router, including:

(a) Technical specifications for hiding connections from diagnostic tools (`lsof`, `netstat`, `ps`)
(b) Any code or configurations implementing such filtering
(c) Deployment date and authorization
(d) Government-agency involvement in development or deployment
(e) Process-specific filtering (e.g., Chrome vs. Safari differential)
(f) Destination-specific filtering (e.g., `10.0.0.1` vs. other destinations)
(g) Integration with macOS kernel or network drivers
(h) Any malware, rootkit, or kernel extension deployed to customer hosts via CPE

REQUEST NO. 29: All documentation regarding systems permitting DHCPv6 provisioning to report "Completed" status despite CRITICAL "Missing Required Option" errors, including:

(a) Configuration-validation bypass procedures
(b) Success-status override capabilities and authorization
(c) Code or configurations implementing the override of CRITICAL errors
(d) When the override capability was added to the TR-069 ACS system
(e) Legitimate use cases for overriding CRITICAL missing-required-option errors
(f) Logs showing validation bypass on October 29, 2025 at 19:49:14
(g) Technical explanations for suppression of Option 82 (Relay Agent Information) and Option 24 (Domain Search List) observed in Plaintiff's forensic capture

CATEGORY G: DNS MANIPULATION CAMPAIGN

REQUEST NO. 30: All DNS query logs, hijacking configurations, and deployment records for DNS manipulation affecting Plaintiff's service during the relevant period, including:

(a) Complete list of domains redirected to `10.0.0.1` (router internal address) on October 29, 2025
(b) The full record of 13,989 DNS anomalies documented in Ex. D-23 at p. 125, l. 9
(c) Technical explanation for each domain's redirection
(d) Standard DNS-proxy configuration compared to the manipulation-active configuration
(e) Authorization records for the manipulation deployment
(f) Duration of manipulation (deployment timestamp through restoration timestamp)

(g) Any TLS proxy, certificate manipulation, or man-in-the-middle infrastructure activated during the same period

Evidentiary predicate: Ex. D-23 at p. 125, l. 9 documents 13,989 DNS anomalies targeting AI-platform domains.

REQUEST NO. 31: All documentation of selective DNS hijacking criteria applied during the relevant period, including:

(a) Which domain categories were subject to hijacking
(b) Which domains were resolved normally
(c) Decision-making rules for the selection
(d) Any indication that legal-services, government-services, or corporate-litigation domains were specifically targeted for hijacking

REQUEST NO. 32: All DNS-over-HTTPS (DoH) infrastructure records associated with Comcast's DoH deployment, specifically `cloud-doh-ch-az2-prod-16p-877085.sys.comcast.net` (IP `96.106.7.238`), including:

(a) Traffic logs for DoH queries originating from Plaintiff's IP range
(b) Any RST injection activity originating from the DoH infrastructure
(c) Query-response latency anomalies
(d) Any correlation between DoH queries and subsequent email-delivery failures

Evidentiary predicate: Ex. D-21 at p. 117, l. 20 documents DoH RST injection paired with email-delivery failure; Ex. D-21 at p. 117, l. 20 includes the 1-microsecond FIN-to-RST gap signature.

REQUEST NO. 33: All documentation regarding IPv6 protocol blocking applied to Plaintiff's service on October 29, 2025, including:

(a) Complete firewall logs showing 244 blocked IPv6 packets (82 at 19:58:00; 162 at 20:28:32)

(b) Firewall rule configuration enabling the blocking

(c) Technical explanation for blocking IPv6 despite advertising "Dual Stack" capability during router initialization

(d) Standard firewall configuration compared to October 29 blocking configuration

(e) Duration of blocking and restoration procedures

(f) Relationship between IPv6 blocking and the DNS hijacking described in REQUEST NO. 30 *supra* (specifically, whether IPv6 blocking prevented IPv6 DNS bypass of the hijacking)

CATEGORY H: DOH-LAYER RST INJECTION

REQUEST NO. 34: All operational records, configuration logs, and packet captures regarding the application-layer localhost RST attack documented in Ex. D-14 at p. 60, l. 31 (5,544 RSTs from `127.0.0.1:9229`), including:

(a) Any Comcast-originated or Comcast-routed traffic that contributed to the localhost artifact

(b) Any CPE-originated packets claiming `127.0.0.1` as source

(c) Firmware functions capable of such origination

REQUEST NO. 35: All logs of router-originated RST traffic targeting IMAP, SMTP, or Apple Push Notification Service destinations from Plaintiff's CPE, including the 100-RST email/push-notification blocking event documented in the forensic record (October 29, 2025 surge).

REQUEST NO. 36: All records of similar incidents across all Comcast customer accounts during the relevant period, including:

(a) One-second shadow administrative sessions with dual authentication

(b) TR-069 password changes immediately before user administrative access

(c) DNS hijacking affecting hundreds of domains

(d) DHCPv6 Option 82/24 suppression with success-status override

(e) Kernel-level connection filtering deployment

(f) IPv6 blocking despite Dual Stack advertisement

Production shall include statistical analysis: total customer accounts affected versus the subset of those accounts in active federal litigation against Comcast or any co-defendant of Comcast in this case.

PHASE 4: VMWARE ATTACK PLATFORM (SMOKING GUN — 30 DAYS)

CATEGORY I: VM IDENTIFICATION (MAC 00:0c:29:50:89:f1)

Note: Requests in this category are directed to Comcast as the ISP whose network carried the attack-platform traffic and as the custodian of any Comcast-side records. Parallel requests are directed to VMware, Inc. as third-party custodian of the MAC-address allocation.

REQUEST NO. 37: All netflow, packet-capture, or DHCP-lease records reflecting devices with MAC address `00:0c:29:50:89:f1` on any Comcast-operated network segment during the relevant period, including:

(a) Lease timestamps and assigned IP addresses

(b) Source-IP and destination-IP pairs for traffic originating from or terminating at this MAC

(c) Correlation with Plaintiff's IP range or with the backbone injection events in Ex. D-1 at p. 3, l. 1

Evidentiary predicate: Ex. D-3 at p. 13, l. 29 identifies this MAC as a VMware-allocated OUI (`00:0c:29` = VMware, Inc.) and documents its presence during the May 24, 2025 attack phase. The VM IP `192.168.8.171` is internal to an attacker-controlled subnet. Supports Compl., Count V (42 U.S.C. § 1985 Conspiracy).

REQUEST NO. 38: All records of any Comcast customer-premises equipment or Comcast backend system that observed, logged, or responded to the VMware VM at MAC `00:0c:29:50:89:f1`, including:

(a) Internal mDNS records (related to the targeting documented in Ex. D-3 at p. 13, l. 29)
(b) ARP tables at CPE showing the MAC's presence
(c) Any alerts or anomaly-detection output flagging the VM's activity
(d) Any administrative actions taken in response to the VM's presence

REQUEST NO. 39: All communications, tickets, or investigation records referencing:

(a) MAC address `00:0c:29:50:89:f1`
(b) IP address `192.168.8.171`
(c) Any VMware-allocated MAC (OUI prefix `00:0c:29`, `00:50:56`, or `00:05:69`) in association with Plaintiff's account or IP range
(d) The "smoking gun" finding in Ex. D-3 at p. 13, l. 29

REQUEST NO. 40: All records regarding Comcast's policies and operational practices when an attack platform is identified on or adjacent to a customer network, including:

(a) Whether customer notification is required
(b) Whether law-enforcement referral is required
(c) Whether Comcast continued routing the attack platform's traffic after observation
(d) Any decision-making recorded in Plaintiff's case

CATEGORY J: VMWARE, INC. ORGANIZATIONAL ROLE (PARALLEL REQUEST TO VMWARE)

Note: Comcast is asked to produce communications with VMware, Inc. on the following topics. VMware, Inc. is served independently as a third-party custodian.

REQUEST NO. 41: All communications between Comcast and VMware, Inc. (including its corporate parent Broadcom, Inc.) during the relevant period regarding:

(a) Traffic analysis or packet-capture data from Comcast networks
(b) Identification of attack platforms or anomalous VMs
(c) Cooperation in lawful-intercept or content-filtering operations
(d) Plaintiff, Plaintiff's IP range, or the VM at MAC `00:0c:29:50:89:f1`

REQUEST NO. 42: All documents reflecting contractual or operational relationships between Comcast and VMware / Broadcom relating to network security, traffic analysis, or packet injection.

REQUEST NO. 43: All communications or documents reflecting Comcast's knowledge of VMware-allocated MAC addresses being used for packet injection, spoofing, or other network attacks against Comcast customers during the relevant period.

PHASE 5: NF-31 × D-33 TOKEN AMPLIFICATION (30 DAYS)
CATEGORY K: ISP THROTTLING × ANTHROPIC API RETRY

REQUEST NO. 44: All records of bandwidth throttling, traffic shaping, or QoS manipulation applied to Plaintiff's IP range during the relevant period, including:

(a) Policy configuration (per-customer or per-destination throttling)
(b) Throttle ratios applied (e.g., the 98% throttle documented in Ex. D-33 at p. 200, l. 7)
(c) Duration and time-of-day distribution
(d) Authorization records for the throttling

(e) Whether throttling was applied selectively to Anthropic-bound traffic versus other destinations

Evidentiary predicate: Finding NF-31 (Ex. E-35, Finding NF-31) documents that when ISP throttling pushes Anthropic API streaming past its 90-second idle timeout (`claude.ts:1877`), Anthropic's non-streaming fallback re-sends the entire prompt, resulting in deterministic 2× billing. Anthropic's own source code comment at `claude.ts:2464-2468` acknowledges "the mid-stream fallback causes double tool execution... See inc-4258." This request develops the ISP-side record of the mechanism's preconditions. **Counts developed:** Compl., Count IX (Breach of Contract), Compl., Count X (Consumer Protection / Deceptive Trade Practices), Compl., Count XII (ECPA, 18 U.S.C. § 2511).

REQUEST NO. 45: All communications, internal memoranda, or operational tickets regarding throttling applied to AI-platform traffic generally, or to Anthropic-bound traffic specifically, during the relevant period.

REQUEST NO. 46: All documentation of Comcast's knowledge of streaming-timeout-to-non-streaming-fallback mechanisms in AI-platform APIs, including:

(a) Any engineering analysis of how Comcast's throttling policies interact with Anthropic's API streaming behavior

(b) Any communication with Anthropic PBC regarding this interaction

(c) Any acknowledgment of the billing consequence documented in Anthropic's source code

REQUEST NO. 47: All packet captures or netflow records sufficient to establish, for each day during the relevant period, the round-trip-time (RTT) and effective

bandwidth between Plaintiff's IP range and `api.anthropic.com`, correlated with whether Plaintiff's client invoked the non-streaming fallback on that day.

PHASE 6: ORGANIZATIONAL SUPPRESSION (30 DAYS)

CATEGORY L: LESRC AND CIRCULAR-REFERRAL PROCEDURES

REQUEST NO. 48: All communications, tickets, and internal records regarding Plaintiff's October 30, 2025 escalation of router compromise, including:

(a) Complete record of the escalation path and referrals among Customer Security Assurance, XFINITY Support, and Corporate offices

(b) Any communication containing the phrases "evidence seizure," "information gets deleted," or substantively similar warnings

(c) The technical basis, if any, for the "information gets deleted" warning

(d) Any coordination with counsel or law enforcement following Plaintiff's escalation

Evidentiary predicate: Ex. D-30 at p. 160, l. 7 documents Comcast's organizational suppression ("circular suppression") response to Plaintiff's reports.

REQUEST NO. 49: All training materials, standard operating procedures, and scripts used by Comcast customer-service or Customer Security Assurance representatives regarding:

(a) Handling customer reports of router compromise or unauthorized administrative access

(b) Evidence-preservation procedures when law-enforcement investigation is possible

(c) Escalation protocols when a customer explicitly references active federal litigation against Comcast

(d) Use of "evidence seizure" or "information gets deleted" language in customer interactions

Production shall include dates training was administered and identification of the individuals who handled Plaintiff's October 30, 2025 contacts.

PHASE 7: LEGAL PROCESS AND GOVERNMENT COORDINATION (IMMEDIATE)

CATEGORY M: NSL / FISA / COURT ORDER / EMERGENCY DISCLOSURE

REQUEST NO. 50: All National Security Letters, FISA orders, court orders, warrants, subpoenas, or emergency disclosure requests related to Plaintiff's service (account associated with Serial `21V4H5FHDA00031`) during the relevant period, including:

(a) Complete text of each legal-process document

(b) Supporting affidavits or probable-cause statements

(c) Judicial findings or authorizations

(d) Scope of surveillance or data collection authorized

(e) Comcast's response and information provided

(f) Any gag orders or nondisclosure requirements

REQUEST NO. 51: All communications between Comcast LESRC and any government agency regarding Plaintiff or Plaintiff's IP range during the relevant period, including:

(a) Communications with FBI

(b) Communications with NSA or other intelligence agencies

(c) Communications with FCC regarding surveillance authorization

(d) Communications with the Executive Office of the President

(e) Any informal requests or coordination outside formal legal process

REQUEST NO. 52: All documents sufficient to establish whether any of the following occurred without a judicial warrant, NSL, FISA order, or emergency exception recognized by statute:

(a) The October 29, 2025 one-second shadow administrative session
(b) The DNS hijacking campaign documented in Ex. D-23 at p. 125, l. 9
(c) The IPv6 blocking documented in REQUEST NO. 33 *supra*
(d) The kernel-level connection filtering capability documented in REQUEST NO. 28 *supra*
(e) The selective throttling documented in Ex. D-33 at p. 200, l. 7

If any of these was performed under color of authority other than formal legal process (including informal agency request, standing policy, or executive direction), produce the authorization documents.

PHASE 8: PERSISTENT CROSS-LAYER IDENTIFICATION SURVIVING VPN DEFENSES (30 DAYS)

Counts developed by this Phase: Compl., Count V (1985(3) Conspiracy), Compl., Count XII (ECPA), Compl., Count IV (Equal Protection).

CATEGORY N: SUBSCRIBER-LINE TRAFFIC CLASSIFICATION SURVIVING DEFENSIVE HARDENING

REQUEST NO. 60: Complete records of all DPI, deep-packet-inspection, and traffic-classification systems applied to Plaintiff's subscriber line (Comcast IP `75.73.199.137` and any other Plaintiff-assigned IP within Plaintiff's CGNAT-assigned range during the relevant period), including: (a) the rule sets, signature definitions, and ML or statistical classifier inputs used by each such system; (b) the daily classifier-output records for Plaintiff's traffic; (c) any classification rules specifically targeting

WireGuard UDP traffic, Mullvad VPN endpoint addresses, or AI-platform destination IPs; (d) the cross-correlation, if any, between Plaintiff's classifier output and the throttling, RST injection, or selective service degradation documented at Ex. D-33 at p. 200, l. 7 and Ex. D-34 at p. 217, l. 18.

Evidentiary predicate: Pleading ¶ 99 (cross-layer identification supplement); App. P, § V.A; Ex. E-35, Finding NF-33 (persistent identification of Plaintiff's Anthropic-bound traffic survived VPN rotation, MAC rotation, NTP leak prevention, DNS-in-VPN encryption, and per-device tunnel routing — proving identification operates through a channel that crosses the VPN encryption boundary). The 188,479 cleartext Anthropic packets visible to Comcast across 143 of 710 hardware-TAP capture segments establishes ISP-side observability material to NF-33 Channel (i) (backbone correlation) and Channel (iv) (encrypted-traffic ML fingerprinting).

REQUEST NO. 61: All records of cleartext metadata retained by Comcast for Plaintiff's traffic during the relevant period, including: (a) TLS Server Name Indication values (Plaintiff's hardware TAP captured 323 unique TLS SNI domains exposed across 209 of 710 capture segments); (b) destination IP records (Plaintiff's hardware TAP captured 891 unique destination IPs exposed in cleartext); (c) DNS query records (the seven-resolver pattern documented at Ex. D-34 at p. 217, l. 18); (d)

Datadog-IP `34.149.66.137` cleartext SNI observations on Plaintiff's physical link (the 44 segments documented at hardware TAP).

Evidentiary predicate: Pleading ¶ 130 (Compl. ¶ 142 cross-layer identification); Ex. E-35, Finding NF-33; Ex. D-34 at p. 217, l. 18.

REQUEST NO. 62: All records of any pre-loaded VPN-endpoint-mapping inventory or persistent VPN-endpoint-identification database used by Comcast against Plaintiff's traffic during the relevant period (NF-33 Channel iii — sustained targeted surveillance predating Plaintiff's defensive hardening), including: (a) the date the mapping was created; (b) the source of the mapping data (whether internally derived, purchased, or received from another carrier or government entity); (c) the technical mechanism by which Plaintiff's WireGuard endpoints were identified despite Plaintiff's repeated server-side peer rotation across all four tunnels (Apr 13 02:15:30-02:20:16 UTC full-fleet rotation documented at Ex. D-34 at p. 217, l. 18).

REQUEST NO. 63: All cross-defendant data-flow records, contracts, technical-cooperation agreements, mutual-information-sharing arrangements, or subprocessor-inheritance routes by which Comcast either (a) transmits Plaintiff-identifying information to Anthropic PBC, Datadog, Inc., or any subprocessor in the Anthropic-Datadog DPA inheritance chain (NF-33 Channel ii — destination-side information transfer carrying `X-Claude-Code-Session-Id` (NF-23) and the twelve-field

GrowthBook payload (NF-35, NF-47)) or (b) receives Plaintiff-identifying information from any of those entities.

Evidentiary predicate: Pleading ¶ 6 (Compl. ¶ 6); App. P, § V.B; Ex. E-35, Finding NF-23; Ex. E-35, Finding NF-35; Ex. E-39, Finding NF-47.

PHASE 9: EXPERT DECLARATION AND DEPOSITION PREPARATION

The following are not discovery requests but notice of expected post-production steps, included so Comcast's production plan can accommodate:

- **Expert declaration on Comcast router forensics.** Plaintiff intends to retain an expert witness on TR-069 ACS operation, Arris/Technicolor firmware, and RST injection tool fingerprinting. Comcast's production should include sufficient technical detail (firmware source, ACS schemas, log-file formats) for third-party expert analysis.
- **Depositions noticed.** Upon completion of document production, Plaintiff intends to notice depositions of: (a) the LESRC custodian responsible for Plaintiff's account period; (b) the TR-069 ACS operations lead for the Minneapolis region; (c) the engineer identified as authorizing any of the October 29, 2025 configuration actions.

PRODUCTION TIMELINE (DRAFT)

Phase	Category	Days from Order
1	A (Datadog IP)	21
2	B (Level 3 / Lumen)	21
2	C (JUMPSTART-2)	21
2	D (Attack fingerprinting)	21
3	E, F, G, H (TR-069 / Router / DNS / DoH-Layer RST)	IMMEDIATE — preservation critical
4	I, J (VMware)	30
5	K (NF-31 / throttling)	30
6	L (Organizational)	30
7	M (Legal process)	IMMEDIATE — preservation critical
8	N (Persistent cross-layer ID)	30

9	(Expert declaration / deposition notice; not a request phase)	n/a

PRESERVATION NOTICE

This request serves as express notice under Federal Rule of Civil Procedure 37(e) that Defendant Comcast Cable Communications, LLC is on notice of the following categories of electronically stored information (ESI) subject to preservation obligation:

1. All TR-069 ACS backend logs for router Serial `21V4H5FHDA00031` and any successor equipment on Plaintiff's account.

2. All netflow, packet-capture, or DPI records for Plaintiff's IP range, including any CGNAT-assigned IP within `68.80.0.0/13`.

3. All communications, tickets, and alerts regarding Plaintiff's account, IP range, or destination traffic to Anthropic, Apple, or OpenAI infrastructure.

4. All firmware versions, configurations, and source code for customer-premises equipment deployed to Plaintiff's service during the relevant period.

Routine destruction of these categories pending resolution of this discovery is expressly prohibited.

Respectfully submitted,

/s/ Joseph Kirchner

Joseph Kirchner
Pro Se Plaintiff
4440 Parklawn Avenue #203
Edina, MN 55435
Telephone: (612) 552-2122
Email: legal@lawsofexistence.com

Dated: May 5, 2026

CERTIFICATE OF SERVICE

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

/s/ Joseph Kirchner_____
Joseph Kirchner
Pro Se Plaintiff