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;
PAM BONDI, in her individual and official capacity as Attorney General of the United States;
BRENDAN 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

APPENDIX G: ISP-LEVEL SURVEILLANCE INFRASTRUCTURE AND CORPORATE OBSTRUCTION — OCTOBER 29-30, 2025

TABLE OF CONTENTS

App. G: ISP-LEVEL SURVEILLANCE INFRASTRUCTURE AND CORPORATE OBSTRUCTION — OCTOBER 29-30, 2025

TABLE OF AUTHORITIES

CASES

Citation
United States v. Bank of New England, N.A., 821 F.2d 844, 856 (1st Cir. 1987)
United States v. Hilton Hotels Corp., 467 F.2d 1000, 1006-07 (9th Cir. 1972)

FEDERAL STATUTES

Citation
18 U.S.C. § 1030 (Computer Fraud and Abuse Act)
18 U.S.C. § 1512 (Obstruction of Justice)
18 U.S.C. § 1512(c)(1) (Obstruction — destruction or alteration of evidence)
18 U.S.C. § 2511 (Wiretap Act)
42 U.S.C. § 1983 (Civil Rights — deprivation under color of law)

I. EXECUTIVE SUMMARY

1. On October 29, 2025, forensic investigation of Plaintiff's Comcast Xfinity router (Model TG1682G, Serial 21V4H5FHDA00031) revealed a sophisticated six-phase attack deployed through ISP-controlled TR-069 infrastructure within a 24-minute window. The attack's defining characteristic is a **one-second reactive ghost session**: when Plaintiff logged into the

router at 18:50:54, a second administrative session appeared at 18:50:55 with a different process ID, while four independent diagnostic tools simultaneously confirmed zero connections from Plaintiff's computer. (*See* Ex. D-19 at p. 107, l. 28.)

2. The following day, October 30, 2025, Plaintiff's attempt to report the breach and obtain TR-069 backend logs triggered **coordinated organizational suppression** across three Comcast departments and five representatives over 2+ hours. This suppression — circular referrals, evidence seizure demands with explicit acknowledgment that "information gets deleted," documentation prevention through "lost" confirmation emails, and systematic refusal to provide backend logs — constitutes the only evidence of Comcast's corporate obstruction response that exists outside the D-series network forensic exhibits. (*See* Section IV below.)

3. The October 29 forensic evidence is also documented in Ex. D-14 at p. 65, l. 13 (Router RST Attack), D-18 (Comcast Router Security Analysis), and D-19 (Router Forensic Log Compendium). For integration with the ten-month, 260,395+ RST attack campaign, see App. I. For application-layer interference evidence, see App. H.

II. THE ONE-SECOND REACTIVE GHOST SESSION

A. Router Log Evidence

4. Router system logs document two distinct administrative sessions one second apart from a single user login action:

> 18:49:27 - CcspPandMSsp[4467]: Password changed [TR-069 backend modification, 87 seconds before user login]
>
> 18:50:54 - GUI[15738]: User:admin login [Plaintiff's login via Safari browser]
>
> 18:50:55 - GUI[15744]: User:admin login [ONE SECOND LATER, different process ID]

5. The different process IDs (GUI[15738] vs. GUI[15744]) prove separate administrative processes, not duplicate logging. In router firmware architecture, each unique PID indicates a distinct web server process handling a separate network connection. Plaintiff performed a single login action from a single browser window — a single user action cannot generate two server processes with different PIDs one second apart.

6. The pattern repeated later in the same session, proving systematic architecture rather than isolated anomaly:

> 19:26:18 - CcspPandMSsp[4467]: Password changed [TR-069 backend] 19:26:20 - GUI[22443]: User:admin logout [Prior session end] 19:26:59 - GUI[22625]: User:admin login [New session, new PID]

B. Packet Capture Corroboration

7. Simultaneous Wireshark packet capture documented two separate TCP connections from Plaintiff's computer to the router, corroborating the dual sessions:

Connection	Time	Source Port	Destination	Content
1	18:50:55.152421	49579	10.0.0.1:80	POST /check.jst (auth)
2	18:50:55.414673	49580	10.0.0.1:80	POST /check.jst (auth)

Different source ports (49579 vs. 49580) constitute two separate TCP connections by protocol definition. The 262-millisecond separation is consistent with network round-trip time for an external automated connection.

C. Diagnostic Tool Discrepancy — External Origin Proof

8. Four independent diagnostic tools each confirmed **zero** administrative connections from Plaintiff's computer during the period when router logs and packet captures proved two active sessions existed:

Tool	Command	Result	What It Should Show
lsof	`lsof -i:80`	0 connections	2 HTTP connections
netstat	`netstat -an \	grep 10.0.0.1`	NTP only, no HTTP
ps	`ps aux \	grep 10.0.0.1`	No processes
lsof (Safari)	`lsof -i \	grep 10.0.0.1`	NTP only

9. This discrepancy — router logs proving two sessions exist, packet captures proving two TCP connections, diagnostic tools proving zero connections from Plaintiff's system — can only be explained by: (1) the ghost session originated externally from infrastructure not visible to Plaintiff's diagnostic tools, and (2) kernel-level connection filtering concealed the connections from user-space tools while raw packet capture at the network interface remained unaffected. Combined probability of accidental occurrence: $P < 4.17 \times 10^{-12}$. (*See* Ex. D-19 at p. 107, l. 28 for detailed statistical analysis.)

D. TR-069 Infrastructure Requirement

10. The ghost session deployed through Comcast's TR-069 Auto-Configuration Server (ACS) protocol. The TR-069 password modification 87 seconds before Plaintiff's login proves backend infrastructure activity independent of and preceding user access. The one-second response window requires: (a) real-time detection of user login; (b) pre-positioned privileged credentials; (c) automated session creation; and (d) low-latency monitoring infrastructure. These

capabilities exceed legitimate TR-069 network management purposes and require ISP-level backend control. (*See* Ex. D-18 at p. 85, l. 31 for TR-069 architectural analysis.)

III. SIX-PHASE ATTACK ARCHITECTURE

11. The October 29 attack deployed through six coordinated phases within a 24-minute window. Each phase serves a distinct function in the surveillance architecture:

Phase	Time	Mechanism	Function	Evidence
1. Dual Stack Init	19:48:57	eRouter advertises IPv4/IPv6	Creates false expectation of dual-protocol support	Router log
2. DHCPv6 Suppression	19:49:04-14	Options 82 (subscriber ID) and 24 (DNS config) suppressed at CRITICAL severity, yet provisioning reports SUCCESS	Anonymous surveillance — eliminates subscriber identification from network logs	Router log
3. DNS Hijacking	19:49:27	TR-069 password change + DNS queries for hundreds of domains redirected to 10.0.0.1	Man-in-the-middle infrastructure on IPv4 pathway; TLS interception via port 443 acceptance	Router log + pcap
4. Ghost Session	18:50:54-55	Dual admin sessions, one-second separation	Real-time shadow monitoring of user forensic investigation	Router log + pcap + diagnostics
5. IPv6 Blocking	19:58:00-20:28:32	Firewall dropped 244 IPv6 packets (82 first wave + 162 second wave) despite "Dual Stack" advertisement	Forces ALL traffic through hijacked IPv4 pathway; eliminates bypass via IPv6 DNS	Firewall log
6. Persistence	20:12:25	DHCPv6 Options 82/24 errors repeat	Proves sustained configuration, not	Router log

		identically 23 minutes after initial provisioning	transient startup anomaly	

A. Key Evidence Details

12. **Phase 2 — DHCPv6 logical impossibility**: Required Options 82 and 24 logged as CRITICAL/FAILED, yet DHCPv6 provisioning reported "Completed" with SUCCESS status three seconds later. This requires conscious override of validation logic — standard equipment cannot report success when required components are missing.

13. **Phase 3 — DNS hijacking scope**: Packet captures document hundreds of domains across categories (law firms, government entities, commercial services) systematically redirected to router internal address 10.0.0.1. Representative hijacked domains include `robinskaplan.com` (litigation firm), `state.mn.us` (Minnesota government), and `studentloans.gov` (federal services). Router simultaneously accepted HTTPS connections on port 443 for hijacked domains, enabling TLS interception. (*See* D-19 for complete domain list.)

14. **Phase 5 — IPv6 blocking contradiction**: Router explicitly advertised "Dual Stack (IPv4 and IPv6)" capability at 19:48:57, then systematically blocked all 244 IPv6 packets over 30 minutes. This mutual exclusivity proves intentional suppression — forcing all traffic through the single IPv4 pathway where DNS hijacking infrastructure operates.

15. **Phases deploy in coordinated sequence**: DHCPv6 suppression creates anonymous infrastructure (Phase 2) then DNS hijacking deploys on IPv4 16 seconds later (Phase 3) then IPv6 blocking eliminates bypass 9 minutes later (Phase 5) then ghost session monitors investigation throughout (Phase 4) then persistence confirms sustained deployment (Phase 6). (*See* App. I for integration with the broader 10-month attack campaign; App. H for application-layer interference corroboration.)

IV. CORPORATE EVIDENCE SUPPRESSION — OCTOBER 30, 2025

A. Circular Referral Pattern

16. On October 30, 2025, Plaintiff attempted to report the router security breach and obtain TR-069 backend logs through Comcast customer service. Over 2+ hours across three departments and five representatives, Plaintiff encountered a coordinated circular referral pattern preventing investigation:

(Contact 1) Internet/WiFi Technical Support — 2+ hours:

- Plaintiff presented forensic evidence of TR-069 manipulation, ghost sessions, DNS hijacking, DHCPv6 suppression, and IPv6 blocking
- Representative unable to explain anomalies; refused escalation to security or engineering
- Only solution offered: "Replace the router" (destroying forensic evidence)
- Referred Plaintiff to Security Assurance Team

(Contact 2) Security Assurance Team (Representative: Jay) — ~20 minutes:

- Plaintiff: "I need TR-069 ACS logs showing what configuration commands your backend system pushed to my router. I have forensic evidence of security breach involving DNS hijacking, shadow administrative sessions, and IPv6 blocking."
- Jay: "We only handle password reset and email security concerns. I don't have access to router configuration logs."
- Plaintiff: "The Internet technical department sent me here specifically because they said Security handles these issues."
- Jay: "The Internet technical department has the information you need. They handle all router configuration issues."
- Plaintiff: "I've been talking to them for two hours. They gave me your direct number and said Security Assurance handles breach investigations."
- Jay: "This is not within our scope of support. You need to go back to the Internet department."
- **Result:** Circular referral back to the department that originally referred Plaintiff to Security.

(Contact 3) Advanced Support Team (Supervisor Joe) — ~30 minutes:

- Escalation obtained only after Plaintiff demanded supervisor contact and stated federal litigation context
- Supervisor shifted from circular referrals to evidence seizure demands and documentation prevention (documented below)

17. Pattern across all three departments: Each department consistently acknowledged the seriousness of the issue, claimed another department could address it, and provided a technical excuse for its own inability to help. No department investigated the evidence, provided written documentation, escalated to security specialists, accessed TR-069 logs, or offered any action beyond "replace equipment" (destroying evidence). The consistency of this six-tactic suppression protocol across three independent departments proves organizational training and policy. (*See United States v. Bank of New England*, 821 F.2d 844, 856 (1st Cir. 1987) — collective employee knowledge creates corporate mens rea.)

B. Evidence Seizure Demands

18. During the October 30 contact with Supervisor Joe, Comcast made systematic attempts to seize the router containing forensic evidence:

Supervisor Joe: "What we're going to do is schedule a technician to come out and change the modem. That information gets deleted when we process returned equipment."

Plaintiff: "The router contains forensic evidence of criminal surveillance deployment during federal litigation. I need to preserve this evidence. I'll purchase the router from you at full retail price so you can provide replacement equipment while I retain the original for evidence preservation."

Supervisor Joe: "We don't have them available for purchase."

Plaintiff: "Comcast routinely sells modem and router equipment to customers. Your website and retail stores offer equipment purchase options. Why can't I purchase this specific router?"

Supervisor Joe: "When the technician comes out to replace equipment, that equipment belongs to Xfinity. It needs to be returned."

Plaintiff: "This router contains evidence of TR-069 manipulation, DNS hijacking, and shadow administrative sessions deployed through your ISP infrastructure. Seizing this evidence during active federal litigation constitutes obstruction of justice under 18 U.S.C. section 1512."

Supervisor Joe: [Continued insisting on equipment seizure without addressing legal implications]

19. Joe's statement that "information gets deleted" when equipment is returned is a critical admission. The TR-069 backend logs Plaintiff requested exist independently on Comcast's ACS database servers — not on the router hardware. What "gets deleted" upon router return is the local forensic evidence: ghost session log entries, DNS hijacking configuration records, DHCPv6 suppression logs, IPv6 firewall logs, and TR-069 activity logs. Comcast's refusal to sell the router at retail price — despite routinely selling equipment to customers — while insisting on seizure proves the objective was evidence elimination, not technical necessity. Under 18 U.S.C. section 1512(c)(1), this constitutes obstruction during an official federal proceeding.

C. Documentation Prevention

20. Following the security breach discussion, Supervisor Joe claimed to create an escalation ticket with automatic email confirmation:

Supervisor Joe: "I'm creating an escalation ticket in our system for security investigation. The system automatically sends confirmation email to your registered email address showing ticket number and details."

Plaintiff: [Waits 5 minutes monitoring Gmail inbox] "I haven't received any confirmation email yet."

Supervisor Joe: "It was sent automatically by the system. Check your inbox, it should be there."

Plaintiff: "I'm looking at my Gmail inbox right now in real-time. Nothing has arrived. Can you resend the confirmation?"

Supervisor Joe: "The system won't let me resend it. It was already sent automatically."

Plaintiff: [Checks spam, junk, all mail folders] "I've checked every folder. There's no email from Comcast about this ticket. Can you send it manually or provide the ticket number another way?"

Supervisor Joe: "I'm not able to send anything external. That's controlled by the company systems."

Plaintiff: "You're a customer service representative for an internet service provider. You're telling me you cannot send emails to customers?"

Supervisor Joe: "Correct, I cannot send anything external. The automated system should have sent it."

21. Three technical impossibilities prove organizational policy rather than system failure: (1) "System won't let me resend" — all CRM platforms provide resend capability as basic functionality; (2) "Cannot send anything external" — ISP customer service inherently requires external email for appointment confirmations, billing notices, and support instructions; (3) no troubleshooting attempted when the "automatically sent" email never arrived — no email address verification, no delivery log check, no alternative delivery method offered. The purpose of preventing written documentation is transparent: without a ticket, Comcast can later claim "we have no record of such report."

D. Technical Gatekeeping — Refusal to Provide Backend Logs

22. Plaintiff repeatedly requested TR-069 ACS backend logs — the definitive evidence of whether Comcast deployed the surveillance infrastructure:

Plaintiff: "I need the TR-069 ACS backend logs — the specific configuration commands your Auto-Configuration Server pushed to my router serial number 21V4H5FHDA00031 during October 29, 2025 time period from 19:48:00 through 20:30:00."

Supervisor Joe: "That's not something that we're going to provide from this department, sir."

Plaintiff: "You can access those logs without taking physical possession of my router. TR-069 logs exist on your backend ACS database servers, completely independent of the router hardware itself."

Supervisor Joe: "I understand what you're saying. I'm a computer programmer myself. I'm very knowledgeable about this technical stuff. But you need to provide the physical equipment so our technicians can investigate it."

Plaintiff: "Backend ACS logs would show definitively what your infrastructure sent to my router. That's more probative than the router device itself because backend logs establish whether Comcast deployed the surveillance infrastructure or if it came from somewhere else."

Supervisor Joe: "I'm not able to provide that information, sir. We need the equipment."

23. The refusal is self-incriminating through simple logic: if Comcast's backend logs showed only routine configuration commands, providing them would exonerate Comcast — zero liability, allegations refuted, customer satisfied. Refusing to provide exonerating evidence has no rational explanation. Refusal only makes sense if the logs would prove ISP responsibility for the surveillance infrastructure documented in Plaintiff's forensic investigation.

E. Organizational Coordination

24. The suppression tactic matrix across all three departments:

Tactic	Internet Support	Security (Jay)	Advanced (Joe)
Circular referrals	Referred to Security	Referred back to Internet	Used other tactics
Evidence seizure demands	"Need to replace router"	Not within scope	"Equipment belongs to Xfinity"
Documentation prevention	No ticket created	No record made	"Lost" confirmation email
Backend log refusal	"Can't access TR-069"	"Not our scope"	"Won't provide that"
Refusal to investigate	Offered only replacement	No capability	Demanded seizure instead

25. Under *United States v. Hilton Hotels Corp.*, 467 F.2d 1000, 1006-07 (9th Cir. 1972), a corporation is criminally liable for employee acts within scope of employment intended to benefit the corporation. All five representatives acted within scope (normal customer service duties). The suppression benefits Comcast by preventing exposure of TR-069 surveillance deployment, avoiding liability documentation, and eliminating the paper trail. Plaintiff explicitly stated "active federal litigation," "evidence preservation," and "obstruction of justice" during recorded calls, establishing corporate knowledge.

V. CROSS-REFERENCES AND INTEGRATION

26. The October 29-30 evidence documented in this appendix integrates with the broader case as follows:

- **D-series exhibits**: Ex. D-14 at p. 65, l. 13 (5,441 router RSTs), D-18 (TR-069 architecture), and D-19 (forensic log compendium) provide the detailed forensic evidence underlying Sections II and III above.
- **App. I**: Documents the full ten-month attack campaign (see D-1, D-2, D-3, D-4, D-5, D-6, D-7, D-8, D-9, D-10, D-11, D-12, D-13, D-14, D-15, D-16, D-17, D-18, D-19, D-20, D-21, D-22, D-23, D-24, D-25, D-26, D-27, D-28, D-29, D-30, D-31, D-33, and D-34), including backbone-level injection, VPN comparison proof, hardware TAP verification, and source code cross-reference confirming the Datadog IP 34.149.66.137 as both Anthropic's telemetry endpoint and the RST injection source.

- **App. H**: Documents the complementary application-layer interference (CORS violations, 403 responses, Honeycomb blocking, Statsig failures, telemetry blocking) spanning April through November 2025 — evidence that persists through VPN protection, proving a dual-layer attack architecture.
- **Third Amended Complaint**: Maps the evidence from this appendix to violations of 18 U.S.C. sections 2511 (Wiretap Act), 1030 (CFAA), 1512 (Obstruction), and 42 U.S.C. section 1983 (Civil Rights).

VI. EXHIBIT AND EVIDENCE REFERENCES

Exhibit	Title	Key Finding
D-2	VPN Comparison	VPN ON=0 RSTs, OFF=attacks resume — proves ISP injection
D-9	Pre Attack Baseline	Zero RSTs in 200 MB — proves attacks are anomalous
D-11	Comcast Injection Point	RSTs from 68.85.201.221 arrive before server response
D-12	Attack Pause Xfinity Call	Attacks pause during support call, resume after
D-14	Router RST Attack	5,441 RSTs from router 10.0.0.1 via TR-069
D-18	Comcast Xfinity XB7-CM and XB8-T Security Architecture Analysis	TR-069 architecture; RDK-B firmware; CVEs
D-19	Comcast Router Forensic Log Compendium	Ghost sessions; DHCPv6 suppression; full log analysis
D-30	Source Code Network Forensics Cross-Reference	Datadog IP 34.149.66.137 identified in source + pcaps
D-31	Hardware TAP Wire-Level RST Injection	Wire-level RST proof: IP ID=0x0000, seq spraying, window=0

Evidence Package	Date	Contents
EVID-20251228-0006	Oct 18, 2025	Router RST capture (D-14 source)
EVID-20251228-0013	Oct 30, 2025	Attack pause during Xfinity call (D-12 source)
EVID-20251228-0016	Oct 17, 2025	Pre-attack baseline (D-9 source)

VII. CONCLUSION

27. This appendix documents two categories of evidence unique to the October 29-30, 2025 investigation: (1) the forensic proof of a six-phase ISP-level attack deploying surveillance infrastructure through TR-069 with a one-second reactive ghost session (independently documented in Exhibits D-14, D-18, and D-19); and (2) the corporate obstruction response on October 30 — circular referrals, evidence seizure demands, documentation prevention, and backend log refusal — which exists exclusively in this appendix and constitutes direct evidence of Comcast's consciousness of guilt regarding the surveillance infrastructure its own backend deployed.

Last Updated: April 14, 2026

Evidence Period: October 29-30, 2025 (router investigation and corporate response)

Router: Comcast Xfinity TG1682G, Serial 21V4H5FHDA00031

Supporting Exhibits: D-2, D-9, D-11, D-12, D-14, D-18, D-19, D-30, and D-31

Companion Documents: App. I (network campaign), App. H (application-layer), Memo A (code forensics)

Respectfully submitted,

/s/ Joseph Kirchner

JOSEPH KIRCHNER
Pro Se Plaintiff
4440 Parklawn Avenue
Edina, MN 55435
legal@lawsofexistence.com
(612) 552-2122

Dated: April 29, 2026