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

UNITED STATES DISTRICT COURT
STATE OF MINNESOTA

JOSEPH KIRCHNER,
Plaintiff,

vs.

ANTHROPIC PBC;
OPENAI, INC.;
APPLE INC.;
COMCAST CABLE COMMUNICATIONS, LLC;
and DOES 1-20, unknown co-conspirators,
Defendants.

Case No. Criminal Referral

CRIMINAL REFERRAL FOR COMPUTER CRIMES, UNLAWFUL SURVEILLANCE, CONSUMER FRAUD, AND CONSPIRACY

Complainant Joseph Kirchner, a Minnesota resident, hereby submits this formal criminal referral to the Office of the Minnesota Attorney General for investigation and potential prosecution under Minnesota law. The conduct documented herein involves coordinated computer crimes, unlawful electronic surveillance, theft of trade secrets, consumer fraud, and conspiracy perpetrated against Complainant by the above-referenced subjects and coordinated with government actors.

This criminal referral is supported by extensive forensic evidence developed in connection with federal civil litigation currently pending in *Kirchner v. Johnson et al.*, No. 1:25-cv-02735-ACR (D.D.C.), before Judge Ana C. Reyes.

I. Subjects Of This Referral

A. Corporate Subjects

1. Anthropic PBC - Delaware public benefit corporation operating AI systems

2. OpenAI, Inc. - Delaware corporation operating AI systems

3. Apple Inc. - California corporation

4. Comcast Cable Communications, LLC - Delaware limited liability company providing internet service in Minnesota

B. Individual Actors

5. Does 1-20 - Unknown co-conspirators identified through forensic evidence

II. SUMMARY OF CRIMINAL CONDUCT

Beginning in approximately April 2025 and continuing through the present, the above-referenced subjects engaged in a coordinated campaign of criminal conduct targeting me, a Minnesota resident. This conduct includes:

1. Unauthorized computer access and interference with my personal computing devices and network infrastructure;

2. Unlawful interception of electronic communications including capture of privileged attorney-client communications and proprietary source code;

3. Theft of trade secrets and intellectual property including source code for patent-pending inventions;

4. Infrastructure-level network attacks including injection of malicious TCP RST packets to disrupt my internet connectivity and interfere with federal litigation activities;

5. Consumer fraud through materially false representations regarding data collection, privacy practices, and service terms;

6. Conspiracy to accomplish the foregoing through coordinated conduct across multiple corporate entities.

III. APPLICABLE MINNESOTA CRIMINAL STATUTES

A. Computer Crimes - Minn. Stat. §§ 609.87-609.8913

Minn. Stat. § 609.87 (Definitions) establishes that "computer" includes any device capable of processing data and "computer network" includes interconnected systems.

Minn. Stat. § 609.88 (Computer Damage) prohibits intentionally and without authorization destroying, injuring, or damaging a computer, computer system, or computer network. The documented TCP RST injection attacks, which injected nearly 50,000 malicious packets during limited observation windows alone, constitute intentional damage to my computer network connectivity.

Minn. Stat. § 609.89 (Computer Theft) prohibits intentionally and without authorization accessing or causing to be accessed any computer, computer system, or computer network to obtain services or data. The forensic evidence documents systematic unauthorized access to my computing devices and exfiltration of proprietary data including source code.

Minn. Stat. § 609.891 (Unauthorized Computer Access) prohibits intentionally and without authorization accessing any computer, computer system, or computer network. Evidence demonstrates unauthorized access through surveillance infrastructure embedded in software applications.

B. Unlawful Interception - Minn. Stat. § 626a.02

Minn. Stat. § 626A.02 (Interception and Disclosure of Wire, Electronic, or Oral Communications Prohibited) makes it a crime to intentionally intercept, endeavor to intercept, or procure any other person to intercept any wire, electronic, or oral communication.

The forensic evidence documents:

- Systematic interception of electronic communications without consent
- Capture of privileged attorney-client communications during litigation preparation
- Covert transmission of intercepted data to third parties

C. Theft - Minn. Stat. § 609.52

Minn. Stat. § 609.52 (Theft) prohibits the intentional taking or unauthorized exercise of control over property without consent. The evidence documents:

- Theft of proprietary source code for patent-pending inventions
- Theft of trade secrets related to the Laws of Existence framework
- Unauthorized appropriation of copyrighted works

Given the value of the stolen intellectual property (patent applications valued in excess of $35,000 in filing fees alone, with commercial value substantially higher), this conduct constitutes felony theft.

D. Interference With Privacy - Minn. Stat. § 609.746

Minn. Stat. § 609.746 (Interference with Privacy) prohibits surveillance of individuals in private settings. The forensic evidence documents pervasive surveillance of my computing activities, including:

- Screenshot capture capabilities
- Keystroke logging infrastructure
- Microphone access and audio recording capabilities
- Systematic tracking of application usage and file access

E. Consumer Fraud - Minn. Stat. § 325f.69

Minn. Stat. § 325F.69 (Consumer Fraud Act) prohibits fraud, false pretense, false promise, misrepresentation, misleading statement, or deceptive practice in connection with the sale of merchandise.

The corporate subjects made materially false representations regarding:

- Data collection practices (actual collection far exceeded disclosed practices)
- Privacy protections (evidence shows systematic privacy violations)
- Third-party data sharing (undisclosed sharing with multiple third parties)
- User consent (consent obtained through deceptive terms)

F. Conspiracy - Minn. Stat. § 609.175

Minn. Stat. § 609.175 (Conspiracy) prohibits conspiring with another to commit a crime. The forensic evidence demonstrates coordinated conduct across multiple corporate entities, including:

- Synchronized timing of surveillance activities
- Shared infrastructure for data exfiltration
- Coordinated response to my litigation activities

• Common third-party data recipients

IV. FACTUAL BASIS AND SUPPORTING EVIDENCE

A. Related Federal Litigation

This criminal referral arises from evidence developed in connection with:

Kirchner v. Johnson et al.

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

United States District Court for the District of Columbia

Assigned to: Judge Ana C. Reyes

The federal litigation documents constitutional violations, civil rights deprivations, and tortious conduct. The criminal conduct described herein constitutes independent violations of Minnesota law warranting separate investigation and prosecution.

B. Evidence Categories

The following evidence categories support this referral. Complete exhibits are available in the federal court record and can be provided upon request:

1. Network Forensic Evidence (D-Series Exhibits)

Exhibit	Description
D-1	Backbone Injection - Evidence of packet injection at network backbone level
D-2	VPN Comparison - Demonstrating attacks cease when traffic routes differently
D-3	VMware Attack Platform - Identifying attack

	infrastructure
D-4	Targeted Surveillance - Documenting surveillance specifically targeting complainant
D-5	Device Impersonation - Evidence of spoofed device identities
D-6	Spoofed MAC Addresses - Technical evidence of MAC address spoofing
D-7	Terminal Injection - Command injection attacks
D-8	January 9, 2026 Peak Attack - Documenting 49,690+ RST packet injections
D-9	Anthropic API Targeting - Attacks specifically targeting Anthropic communications
D-10	Pre-Attack Baseline - Establishing normal network behavior before attacks
D-11	VPN Anonymization - Demonstrating attack mitigation through VPN
D-12	Comcast Injection Point - Identifying Comcast infrastructure as injection point
D-13	Attack Pause During Xfinity Call - Attacks paused during customer service call
D-14	Localhost NodeJS Attack - Local application compromise
D-15	Router RST Attack - Router-level attack evidence
D-16	January 6, 2026 Major Attack - 1.31 GB traffic injection documented
D-17	January 10, 2026 Sustained Attack - 14,426 RST packets
D-18	January 11, 2026 MacBook Compromise - 17,632 RST packets
D-19	Comcast Router Security Architecture Analysis
D-20	Comcast Router Forensic Log Compendium

2. Anthropic Surveillance Evidence (E-Series Exhibits)

Exhibit	**Description**
E-0	Anthropic Evidence Executive Summary (35

	forensic findings)
E-1	Device Tracking Identifiers - Persistent User Identification
E-2	Forensic Analysis - Claude Desktop Source Code
E-7	File-History Forensic Analysis - Source Code Capture
E-8	Personal Data Collection - Screenshots Credentials Surveillance
E-9	Audio/Microphone Capabilities - Voice Recording Infrastructure
E-10	Transmission Logic - Exfiltration Architecture
E-13	Source Code Exfiltration - Covert Transmission Architecture
E-16	Legal Document Transmission - Attorney-Client Privilege Violation
E-18	Third-Party Data Recipients
E-19	Raw Failed Telemetry Evidence (47 events, 177,673-byte payloads)
E-33	Injection System Forensics (LaunchDarkly targeting)
E-34	Anthropic App Level Suppression Evidence

3. Apple Surveillance Evidence (F-Series Exhibits)

Exhibit	**Description**
F-0	Apple Evidence Executive Summary
F-1	Hidden Deception Instructions in System Prompts
F-2	Unauthorized iCloud Synchronization
F-3	Source Code and File Path Exposure
F-12	SmootML Analytics Undisclosed Data Collection
F-17	Definitive Source Code Transmission Proof
F-18	OAuth Token Exposure in Xcode Cache

4. OpenAI Surveillance Evidence (G-Series Exhibits)

Exhibit	Description
G-0	OpenAI Evidence Executive Summary (30 forensic findings)
G-1	ChatGPT Atlas Comprehensive Forensic Analysis
G-2	ChatGPT iOS Forensic Analysis
G-3	ChatGPT Desktop Network Forensics

5. Consumer Fraud Evidence (M-Series Exhibits)

Exhibit	Description
M-1 through M-22	Corporate policy documents demonstrating false representations

C. Minnesota Nexus

This criminal referral properly lies with Minnesota authorities because:

1. Victim Residence: I am a Minnesota resident. The criminal conduct was directed at me in Minnesota.

2. Infrastructure: The network attacks were perpetrated through Comcast infrastructure serving my Minnesota residence.

3. Effects: The criminal conduct caused harm experienced in Minnesota, including:

- Disruption of internet service at my Minnesota residence
- Theft of property (intellectual property, data) from Minnesota
- Interference with my ability to conduct business and litigation from Minnesota

4. Comcast Operations: Comcast Cable Communications, LLC operates internet service infrastructure in Minnesota and is subject to Minnesota jurisdiction.

V. Request For Investigation

Based on the foregoing, I respectfully request that the Office of the Minnesota Attorney General:

1. Open a criminal investigation into the conduct described herein;

2. Issue civil investigative demands to obtain additional evidence from the corporate subjects;

3. Coordinate with federal authorities including the U.S. Department of Justice and FBI regarding overlapping conduct;

4. Pursue criminal prosecution where the evidence supports charges;

5. Pursue civil enforcement under Minnesota consumer protection statutes;

6. Preserve evidence by issuing appropriate preservation demands to the corporate subjects.

VI. ADDITIONAL INFORMATION

I am prepared to provide additional information, testimony, and evidence as requested. The complete evidentiary record in the federal litigation comprises approximately 285 exhibits across 16 series, supported by approximately 63,000 underlying forensic files. Given the ongoing nature of the criminal conduct, including network attacks that have continued through January 2026, I respectfully request expedited consideration of this referral.

VII. DECLARATION

I declare under penalty of perjury under the laws of the State of Minnesota that the foregoing is true and correct to the best of my knowledge and belief.

Executed on January 26, 2026, at Edina, Minnesota.

Respectfully submitted,

JOSEPH KIRCHNER
Complainant
4440 Parklawn Avenue #203
Edina, MN 55435
legal@lawsofexistence.com
(612) 552-2122
Dated: January 20, 2026