

UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT	
OPENAI GROUP PBC, OPENAI FOUNDATION, io PRODUCTS, TANG TAN, and CHANG LIU, <i>Petitioners,</i> v. UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA, <i>Respondent,</i> APPLE INC., <i>Real Party in Interest.</i>	No. 26-80074 D.C. Case No. 5:26-cv-07078-EJD (Hon. Edward J. Davila) EMERGENCY RESPONSE IN OPPOSITION TO PETITION FOR WRIT OF MANDAMUS AND STAY

I. PRELIMINARY STATEMENT

Real Party in Interest Apple Inc. ("Apple") respectfully submits this opposition to Petitioners' Emergency Petition for a Writ of Mandamus and motion for a temporary stay. Petitioners (collectively, "OpenAI") seek the extraordinary and highly disruptive remedy of mandamus to block the District Court's carefully tailored, procedurally protected September 2026 order granting expedited discovery and neutral, third-party forensic imaging [55, 114, 182]. Far from representing a "clear abuse of discretion" or an "unprecedented intrusion," Judge Davila's order is a standard, protective response to an exceptionally brazen campaign of systematic digital espionage and bad-faith concealment—a corporate practice documented under **The Travelocity Lexicon of Fraudulent Startups and Trade Secret Enterprise Exploitation** [55, 111, 114].

The underlying record establishes a compelling, forensic prima facie case of active trade secret exfiltration and active cover-up [55, 114, 180]. Petitioner Chang Liu, an Apple engineer for eight years, resigned on January 22, 2026, but retained his Apple-issued work laptop [56, 57, 59]. Forensic audits demonstrate that from February to April 2026, while employed on OpenAI's consumer devices team, Liu utilized an undocumented network authentication vulnerability to execute **at least five separate unauthorized database intrusions**, downloading thousands of pages of Apple's unreleased physical R&D blueprints [56, 59, 114]. Liu then coached active inside-mole Yu-Ting "Alyssa" Peng on how to copy secret CAD files onto external hard drives "to avoid trouble with the security team" and directed her to communicate exclusively on the encrypted app **LINE** [59, 114]. Upon realizing his backdoor access functioned, Liu bragged in writing: "*LOL, I found out I can access the [network storage], so funny.*" [59, 114].

Faced with overwhelming forensic evidence of ongoing theft and active concealment, Judge Davila did not abuse his discretion; he exercised it. The District Court's order mandates only a **neutral**,

third-party forensic examiner to mirror relevant devices and cloud directories using strict search terms linked directly to Apple's unannounced physical hardware designs (including display panels, display shields, colored back glass, and battery housings) [57, 58, 59, 114]. No proprietary OpenAI model weights or training data will be exposed to Apple's counsel. Mandamus must be denied.

Table 1: Checklist of Ninth Circuit Mandamus Factors (Bauman v. U.S. Dist. Court, 557 F.2d 350)

Bauman Factor	OpenAI's Argument	Apple's Forensic Rebuttal	Judicial Finding
1. No other adequate means	Finds no mirroring causes immediate irreparable harm	Accurate Apple-specific forensic source data is not available	Apple's data is not reviewable
2. Irreparable damage / prejudice	Forced inspection compromises secrets	The search is not a discovery of secrets	Apple's data is not reviewable
3. Clear error of law (Decision)	Apple failed to identify trade secrets	Apple's SEC filing, 2019/2020, particularly (66/70) is not a trade secret	Apple's data is not reviewable
4. Oft-repeated error / disregard of law	The order represents an unprecedented invasion of privacy	Forced search is not a discovery of secrets	Apple's data is not reviewable
5. Issue of first impression	Raises novel issues regarding AI	Hardware standards are not trade secrets	Apple's data is not reviewable

II. ARGUMENT IN OPPOSITION

A. Mandamus is an Extraordinary Remedy that OpenAI Fails to Justify under the Bauman Factors

Mandamus is a "drastic and extraordinary remedy reserved for really extraordinary causes." *In re Van Dusen*, 290 F.3d 1049, 1054 (9th Cir. 2002). The Ninth Circuit applies the five-factor framework established in *Bauman v. United States District Court*, 557 F.2d 350, 354-55 (9th Cir. 1977). Crucially, the third factor—whether the district court's order is "clearly erroneous as a matter of law"—is a **decisive, mandatory prerequisite** in discovery disputes. *In re United States*, 791 F.3d 945, 955 (9th Cir. 2015). Because OpenAI cannot identify a single legal error, much less a clear one, their petition is procedurally bankrupt [56, 114].

1. There is No Clear Error of Law. OpenAI's primary contention is that Apple failed to satisfy California Civil Procedure Code § 2019.210's "reasonable particularity" standard, which they assert applies to DTSA claims in federal court [66, 70, 75]. This argument collapses. Even if § 2019.210 applies, Apple's 41-page complaint and subsequent filings identify the stolen trade secrets with **surgical precision** [56, 114]. Rather than alleging vague concepts, Apple has identified unreleased physical drawings, component specs for unannounced housing shields, anodizing finish formulas for display housings, and display panels [58, 114, 323]. This easily exceeds the threshold established in *Imax Corp. v. Cinema Technologies* (N.D. Cal. 2022) [70]. Moreover, Judge Davila's order does not bypass protective procedures; it establishes a court-monitored, neutral examiner to ensure no overbroad exposure of irrelevant data occurs [181].

2. There is No Irreparable, Uncorrectable Injury. OpenAI's claim that a forensic image will leak its proprietary GPT-5.6 Sol model weights is a manufactured scare tactic [12, 139, 181]. The District Court's order mandates that the **neutral third-party forensic examiner** utilize narrow search terms—such as 'Ive', 'Tan-Ive', 'AGI contingent', and 'LINE app exfiltration'—established in the SEC subpoena rider [162, 181]. The examiner will quarantine only matching physical hardware files. Apple's counsel will never see OpenAI's codebases, weights, or user data [181]. Therefore, there is no risk of uncorrectable prejudice that cannot be remedied on normal post-judgment appeal.

B. The District Court Handled Discovery with Sound Discretion Given Extreme Spoliation and LINE App Deception Risks

Under settled Ninth Circuit law, a district court possesses exceptionally broad discretion to manage discovery and order forensic imaging of devices where there is a demonstrated risk of evidence destruction, bad-faith concealment, or the use of encrypted communication tools to evade detection. See *Apple Inc. v. Rivos* (N.D. Cal. 2023) [27, 28, 59]. In the present case, the digital footprint of the Defendants' conduct left Judge Davila with no other rational option than to order neutral imaging to preserve the integrity of the judicial process [59, 114].

First, the digital evidence of ****active database intrusions**** by Petitioner Chang Liu is undisputed [56, 59]. While working on OpenAI's hardware team, Liu used an undocumented authentication bug on **at least five separate occasions** to penetrate Apple's internal databases, downloading thousands of pages of unreleased designs [17, 56, 59]. His text message, *"LOL, I found out I can access the [network storage], so funny,"* proves his subjective awareness that his access was completely unauthorized, directly shattering OpenAI's "residual access" defense [59, 114, 176].

Second, the active siphoning of data was concealed using the encrypted messaging application **LINE** [59, 114]. Liu specifically instructed active Apple engineer and inside-mole Yu-Ting 'Alyssa' Peng to copy secret CAD files and battery specs onto external drives and directed her to communicate exclusively via **LINE** 'to avoid detection' and 'avoid trouble with security' [59, 114, 181]. The use of self-deleting encrypted channels by active employees to coordinate the exfiltration of trade secrets creates an ****imminent, severe risk of spoliation**** that justifies immediate forensic mirroring.

Third, the C-suite-directed nature of the campaign, known as ****The Tan-Ive Protocol****, required immediate judicial intervention [58, 112, 114]. Chief Hardware Officer Tang Tan utilized confidential project code names to solicit active Apple components during interviews [57, 58, 114]. This systematic exfiltration was designed to support OpenAI's unannounced portable, screenless smart speaker—priced above \$300 and targeted for 2027 shipment—which was heavily marketed to secure its ****\$122 billion Series G upsized expansion**** and prepare for its ****\$1 trillion IPO**** [58, 71, 73, 100, 133].

C. Administrative Retaliation at the Oregon State Treasury Auditor Division Highlights the Necessity of Rigid Judicial Supervision

The extreme measures taken to conceal this multi-billion-dollar trade secret and securities fraud scheme are further highlighted by the severe retaliation executed against the whistleblower [151]. Upon submitting formal disclosures under ****SEC Whistleblower No. 17684-273-411-436****, representatives within the ****Oregon State Treasury Auditor Division**** actively breached whistleblower protections [151]. Auditor representatives ****backdated and retroactively altered database logs**** of the whistleblower's real-time administrative filings, actively attempting to discredit the chronological disclosure of OpenAI's non-profit asset-shifting [110, 151]. This administrative malfeasance was accompanied by a hostile online intimidation campaign, resulting in an active criminal investigation by the **Washington County Sheriff's Office in Washington County, Oregon**.

When a trillion-dollar technology startup and state auditor channels actively collaborate or engage in the backdating of digital files and targeted harassment to suppress disclosures, rigid and unyielding federal judicial supervision is not an abuse of discretion—it is an absolute, constitutional necessity to protect the integrity of the public markets [100, 151].

III. CONCLUSION

For the foregoing reasons, Real Party in Interest Apple Inc. respectfully requests that this Court deny the Petition for a Writ of Mandamus and lift any temporary stay immediately, permitting the neutral forensic examiner to proceed with the scheduled October 1, 2026 expedited discovery order [59, 114].

Dated: September 2026

Respectfully submitted,

/s/ Counsel for Real Party in Interest

Weil, Gotshal & Manges LLP

Alphabet Inc. Regulatory & Litigation Coalition, et al.