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-11: FOREIGN INFLUENCE — DATADOG ISRAEL LTD., RAFAEL DEVELOPMENT CORPORATION, ELRON VENTURES LTD., AND THE OZCODE PATENT FAMILY

INTRODUCTION

1. Scope and predicate. This DISCOVERY-11 is the consolidated foreign-influence demand schedule supporting App. P (Israeli AI Surveillance Facilitation — Datadog/OzCode Architecture and Personnel Pipeline). The architectural, financial, jurisdictional, and personnel-level findings established at App. P §§ II–VII identify a defined set of corporate, governmental, and individual custodians whose records are necessary for full development of Plaintiff's Counts V (§ 1985(3) Conspiracy), VI (RICO), IX (Breach), X (Consumer Protection), XII (ECPA), XIII (CFAA), and XIV (CCPA). This DISCOVERY-11 enumerates each demand category with the corresponding App. P § cross-reference for evidentiary predicate.

2. Absorption of TAC residual demands. This DISCOVERY-11 absorbs the residual foreign-influence-adjacent discovery demands appearing at Compl. ¶ 135 paragraphs (e) through (g) (Datadog retention logs; Anthropic-Datadog per-user-enablement communications) and at Compl. ¶ 136 (cross-layer terminus demands), which were originally embedded in the Third Amended Complaint and are re-enumerated here with additional primitive-level and Israeli-jurisdictional demands developed across App. P §§ II through VII.

3. Organization. Demands are organized by target entity and named individual. Each demand is framed as a Federal Rule of Civil Procedure 26 / 34 / 45 request. Plaintiff reserves the right to refine demands at the formal discovery stage and to seek additional targeted demands as fact development warrants.

A. Datadog Israel Ltd. as Direct Custodian (Five Demands)

Demand A.1: **Complete employment roster.** Complete employment roster for Datadog Israel Ltd. from September 14, 2021 (incorporation date) through the date of production, with for each employee: (i) prior Israel Defense Forces service, unit, dates, rank, and reservist status; (ii) role at Datadog Israel Ltd.; (iii) scope of access to United States customer data; (iv) current or former status.

Demand A.2: **Records of Israeli-government legal process.** All records of Israeli-government legal process (mandatory-access orders, intelligence requests, subpoenas, search warrants, administrative disclosure orders) directed to Datadog Israel Ltd. during the relevant period (September 14, 2021 through the date of production).

Demand A.3: **Data-flow records.** Complete data-flow records between Datadog Inc. (United States parent) and Datadog Israel Ltd. attributable to every accountUUID in Plaintiff's accountUUID Roster (DISCOVERY-5 §A.0) and to every other Plaintiff-related account identifier within the operator's `Laws of Existence` Anthropic organization (`organization_uuid 2e997389-cf99-41ee-8ee3-764442034332`).

Demand A.4: **Organizational reporting chain.** The organizational reporting chain from Datadog Israel Ltd. to Datadog, Inc., including which functional areas operate primarily under Israeli rather than United States legal authority.

Demand A.5: **Customer-data-class inventory.** Complete inventory of customer data classes accessible to Datadog Israel Ltd. employees in their normal engineering work, including Artificial-Intelligence and Large-Language-Model development work on the IDE AI Experiences product, the Dynamic Instrumentation product, and the `dd-trace-dotnet` observability-ingestion framework.

B. Named Individual — Omer Raviv (Six Demands, Expanded with IDF Unit 8200 Service Detail)

Demand B.1: **Employment history and access scope.** Complete employment history at Datadog Israel Ltd., including role, reporting chain, scope of access to United States customer data (including Anthropic-originated

telemetry processed via `dd-trace-dotnet`), commits, design-document authorship, code-review authority, and hiring authority.

Demand B.2: **IDF Unit 8200 service record.** Prior Israel Defense Forces service: unit, dates, rank, reservist status, and any ongoing reservist obligations as of the date of production. Raviv publicly self-identifies as "veteran commander at the prestigious IDF's 8200 unit"; Plaintiff seeks the complete service record including (i) command tenure dates; (ii) specific roles within Unit 8200; (iii) any ongoing reservist obligations; (iv) any security clearance currently held; (v) any obligations to the Israeli state under the Israeli Reserve Duty Law or analogous authorities.

Demand B.3: **Technical scope within observability-ingestion systems.** Engineering-function scope at Datadog Israel Ltd., specifically: commits, design-document authorship, code-review authority, and access-control posture within the `dd-trace-dotnet` tracing framework and adjacent observability-ingestion systems that process Anthropic Claude Code telemetry routed to endpoint `34.149.66.137`.

Demand B.4: **Communications with OzCode-origin personnel.** All communications between Raviv and any other named former OzCode founder or engineer now employed by Datadog or Datadog Israel Ltd., including Alon Mordechai Fliess, Matan Green, Evgeni Wachnowezki, Shimon Hason, Erez Fliess, and any other former-OzCode individual now at Datadog.

Demand B.5: **Communications with Elron/RDC/Rafael personnel post-acquisition.** All communications between Raviv and any Elron Ventures Ltd. or Rafael Development Corporation or Rafael Advanced Defense Systems Ltd. personnel post-acquisition (October 26, 2021 through the date of production).

Demand B.6: **Communications with Israeli-government entities.** All communications between Raviv and any Israeli-government entity regarding personnel reserve obligations, security clearance, or any intelligence, national-security, or defense-related matter.

D. Named Co-Inventors — Evgeni Wachnowezki and Matan Green (Six Demands)

Demand D.1: **Wachnowezki current employer.** Current employer and role of Evgeni Wachnowezki, named co-inventor on US 2026/0072809 A1 (Code Origin and Runtime Duplicity).

Demand D.2: **Wachnowezki prior OzCode association.** Whether Wachnowezki was an employee, contractor, or consultant of OzCode Ltd. prior to the October 26, 2021 asset sale, and the dates and scope of any such association.

Demand D.3: **Wachnowezki Israeli military service history.** Wachnowezki's Israel Defense Forces service history (unit, dates, rank, ongoing reservist obligations), and any service in Unit 8200, Air Force intelligence, or other military-intelligence units.

Demand D.4: **Green current employer.** Current employer and role of Matan Green, named co-inventor on US 2026/0072809 A1 (publicly

disclosed as Senior Software Engineer at Datadog on Dynamic Instrumentation, and as Israeli Air Force veteran).

Demand D.5: **Green Israeli military service history.** Green's Israel Defense Forces service history (unit, dates, rank, ongoing reservist obligations).

Demand D.6: **Co-inventor communications regarding 2024 continuation.** All communications between Wachnowezki, Green, and Raviv concerning the September 9, 2024 continuation application US 18/828,099 / US 2026/0072809 A1 (Code Origin and Runtime Duplicity), including any communications addressing the "network or system security" branching disclosed at paragraph [0048] of that application's specification.

E. Named Individual — Alon Mordechai Fliess (Five Demands, Expanded with Microsoft Connection)

Demand E.1: **Current employer.** Current employer and role.

Demand E.2: **Continuing role at OzCode Ltd.** Any continuing role at OzCode Ltd. (which may still exist as an Israeli legal entity post-asset-sale).

Demand E.3: **IDF service history.** Prior Israel Defense Forces service history including unit, dates, rank, and any ongoing reservist obligations.

Demand E.4: **Microsoft Regional Director and Microsoft Azure MVP status.** Per Exhibit L-9 (archived oz-code.com leadership page, October 21, 2019 Wayback Machine capture), at the time of the January 7, 2019 OzCode patent filings, Fliess held both Microsoft Regional Director status and Microsoft Azure MVP designation. Plaintiff seeks: (i)

Fliess's complete history of Microsoft Regional Director status, including initial appointment date, reappointment dates through the present, and any continuing relationship with Microsoft Corporation as Microsoft Regional Director or in any other capacity; (ii) Fliess's complete history of Microsoft MVP and Azure MVP status, including award years and any continuing recognition; (iii) any consulting, advisory, contractual, or compensation relationship between Fliess and Microsoft Corporation from January 2019 through the present; (iv) any Microsoft strategic-roadmap briefings Fliess received as Microsoft Regional Director that informed the January 7, 2019 OzCode patent specifications; (v) any communications between Fliess and Microsoft Azure architecture personnel during the patent prosecution and post-prosecution period (January 2018 through the present).

Demand E.5: **OzCode-Microsoft architectural relationship.** Any commercial, technical, or licensing relationship between OzCode Ltd. and Microsoft Corporation, including (i) OzCode product integration with Microsoft Visual Studio,.NET, Azure DevOps, or Azure App Service; (ii) Microsoft technology-partnership programs; (iii) Microsoft enterprise-customer referrals to OzCode; (iv) Microsoft licensing of OzCode time-travel-debugger technology; (v) any post-acquisition Datadog-Microsoft relationship inheriting OzCode-era arrangements; (vi) any familial relationship between Alon Mordechai Fliess and Erez Fliess (separate-individual OzCode Co-Founder & Chairman) and the

role of any familial relationship in OzCode's founding capital structure or post-acquisition continuing-equity arrangements.

F. Named Individual — Yair Cohen / "Cohan" (Three Demands)

Demand F.1: **Datadog employment history.** Complete employment history at Datadog, including role, reporting chain, scope of access to Anthropic-related customer data (including Plaintiff's data), and separation date (if separated).

Demand F.2: **Temporal relationship to Sentra founding.** Whether access to Anthropic-related customer data preceded his Sentra co-founding activity in July 2021, and whether any portion of that access persisted after his departure.

Demand F.3: **Communications with Sentra co-founders.** All communications between him and any Sentra co-founder (Asaf Kochan, Ron Reiter, Yoav Regev) during his Datadog tenure.

G. Datadog Israel Ltd. — Post-Hason Successor and Continuing-Relationship Records (Four Demands)

Demand G.1: **Successor identity.** Identity, appointment date, and role of the successor to Shimon Hason as Head of Datadog Israel Ltd. (or equivalent senior role). Hason departed Datadog Israel Ltd. on or about March 17, 2025 to become Chief Executive Officer of Incredibuild; no publicly-announced successor has been identified by

Plaintiff in Israeli business press or on public LinkedIn as of the date of this Request.

Demand G.2: **Hason transition records.** All Datadog and Datadog Israel Ltd. internal communications, organizational charts, public-affairs materials, and personnel records documenting the timing, scope, and management of the Hason departure and successor onboarding, including any temporary acting-leadership arrangement during the interregnum.

Demand G.3: **Successor's employment terms and reporting chain.** Successor's employment terms, scope of responsibility for Datadog Israel Ltd. operations, scope of access to Anthropic-related customer data (including Plaintiff's data), and reporting chain to Datadog, Inc. (Delaware).

Demand G.4: **Continuing relationship between Hason and Datadog post-departure.** Any continuing contractual, advisory, equity, consulting, or other relationship between Hason and Datadog, Inc. or Datadog Israel Ltd. post-departure, including any Incredibuild–Datadog commercial relationship through which Hason continues to interact with Datadog operations.

H. RDC Co-Chief Executive Officer Transitions and Continuing Rafael Relationships (Three Demands)

Demand H.1: **RDC Co-CEO appointment history.** Complete appointment history of the Rafael-appointed Co-Chief Executive Officer seat at Rafael

Development Corporation Ltd. (RDC) during the relevant period, including all transitions, the dates and durations of each appointment, and the reason for each transition.

Demand H.2: **Yaron Kulas tenure and departure records.** All RDC, Rafael Advanced Defense Systems Ltd., and Rafael Development Corporation Ltd. internal communications, board meeting minutes, organizational charts, and personnel records documenting the tenure of Yaron Kulas as Rafael-appointed Co-Chief Executive Officer of RDC and the circumstances of his departure or reassignment.

Demand H.3: **Kulas-to-Shechter transition.** Complete record of the transition from Yaron Kulas to Liat Shechter as Rafael-appointed Co-Chief Executive Officer of RDC, including: (a) the timing of the transition (which occurred between Elron's August 2025 Investor Deck and the 2025 Annual Report filing date); (b) the reason for reassignment of Kulas; (c) any continuing contractual, advisory, equity, or consulting relationship between Kulas and Rafael, RDC, or any Datadog entity post-transition; (d) Shechter's employment terms, scope of responsibility, prior relationships with Rafael, RDC, OzCode, or Datadog, and Israeli military or intelligence service history.

I. OZCODE ACQUISITION DILIGENCE AND COMMUNICATIONS (FIVE DEMANDS)

Demand I.1: **Datadog's 2021 acquisition diligence file.** Datadog's complete 2021 OzCode acquisition diligence file, including representations and

warranties regarding Rafael intellectual-property licenses, Israeli Ministry of Defense-origin technology, export-control restrictions, and any foreign-government data-access arrangements applicable to OzCode's technology or personnel.

Demand I.2: **Pre-acquisition communications.** All pre-acquisition communications between Datadog, Inc. and Elron Ventures Ltd., Rafael Development Corporation Ltd., Rafael Advanced Defense Systems Ltd., or TPY Capital regarding OzCode, personnel, technology, or any other commercial matter.

Demand I.3: **Post-acquisition communications.** All post-acquisition communications between Datadog, Inc. (and/or Datadog Israel Ltd.) and Elron Ventures Ltd., Rafael Development Corporation Ltd., or Rafael Advanced Defense Systems Ltd., including meetings held at or involving ToHa Tower (114 Yigal Alon Street, Tel Aviv).

Demand I.4: **OzCode board minutes.** OzCode board minutes, shareholder communications, and investor-reporting documents from November 13, 2018 (seed round) through November 4, 2021 (Datadog acquisition close), with specific attention to records involving Yaron Elad (then Elron Vice President and Chief Financial Officer, OzCode board member) and Elik Israel Etzion (then Elron Vice President for Cybersecurity, OzCode board member).

Demand I.5: **Referral and deal-flow records.** Records of any introduction, referral, or deal-flow arrangement between Datadog and Elron

Ventures or Rafael Development Corporation regarding Seekret (2022 acquisition), Upwind Security (attempted-but-not-closed 2025-2026 acquisition), or any other Israeli-company acquisition target.

Demand I.6: **Rafael Advanced Defense Systems Ltd. capital flows to and from Rafael Development Corporation Ltd. during the OzCode ownership window.** All records of capital flows between Rafael Advanced Defense Systems Ltd. ("Rafael") and Rafael Development Corporation Ltd. ("RDC") from November 2018 (OzCode seed round) through the post-close distribution period (October 2021 – 2023), including: (i) Rafael's documented March 2021 $8,000,000 loan to RDC (Elron 2021 Periodic Report Part II §1.2.4; Elron 2025 Annual Report §23.7), including the loan agreement, term sheet, board resolution, and disbursement records; (ii) Rafael's documented 49.9% share of RDC's 2021 aggregate gains (~$8,459,000 per Elron 2021 Periodic Report Part II §1.3.2); (iii) Rafael's OzCode-specific share of RDC exit consideration (~$700,000 per Elron 2023 Periodic Report §3.B.2.q); and (iv) any communications between Rafael, RDC, Elron, or Datadog concerning the timing or amount of any of the foregoing.

J. Acquisition Integration (Two Demands)

Demand J.1: **Engineering-team assignment.** Which engineering teams from OzCode (2021) and Seekret (2022) are now assigned to systems that process Anthropic customer telemetry, and which of those teams are substantially composed of former-IDF personnel.

Demand J.2: **Integration communications.** All communications concerning the integration of acquired companies' engineering practices into Datadog's cloud-security platform, particularly those affecting handling of customer data referenced by per-user GrowthBook force-rules.

K. Israeli Intelligence Coordination (Three Demands)

Demand K.1: **Mandatory-disclosure orders.** Any mandatory-disclosure orders, intelligence-sharing arrangements, or classified-cooperation agreements between Datadog Israel Ltd. and the State of Israel during the relevant period.

Demand K.2: **Communications with IDF units.** Any communications between Datadog Israel Ltd. employees and any Israel Defense Forces unit (whether as current duty personnel, reservist personnel, or as employer-of-record for reserve duty).

Demand K.3: **Records of Israeli state access.** All records of any Israeli state entity accessing Datadog customer data through Datadog Israel Ltd.'s systems or personnel.

L. PATENT FAMILY COMPLETENESS (TEN DEMANDS)

Demand L.1: **Full priority family inventory.** Full inventory of the seven-application priority family in the 2019 OzCode patent family + grant/pending/abandoned status for each.

Demand L.2: **Assignment status and dates.** Assignment status and dates for each patent in the family.

Demand L.3: **Stated consideration.** Stated consideration in the USPTO assignment deed texts for each patent.

Demand L.4: **License-back arrangements.** Any license-back, cross-license, or sublicense arrangements between Datadog, Inc. and OzCode Ltd. (or any successor).

Demand L.5: **Innovation Authority grants.** Innovation Authority "Sponsored Knowledge" grant history for OzCode and any redemption fee paid for transfer of sponsored intellectual property to Datadog, Inc.

Demand L.6: **Cross-licensing with OzCode Ltd.** Any cross-licensing arrangement between Datadog, Inc. and OzCode Ltd. (any retained patents or any continuing license to Datadog-assigned patents).

Demand L.7: **OzCode Ltd. current status.** Current operational status of OzCode Ltd. + shareholder list + board composition + any continuing revenue or licensing streams.

Demand L.8: **Complete October 2021 APA.** Complete October 2021 Asset Purchase Agreement between Datadog, Inc. and OzCode Ltd., including all schedules, exhibits, side letters, and representations-and-warranties addressing intellectual property, personnel transfer, non-competition, and Rafael-technology-license continuity.

Demand L.9: **Recordation-timing communications.** All internal communications between and among Datadog, Inc., OzCode Ltd., the Israel Innovation

Authority, and the Israeli Tax Authority concerning the timing of USPTO recordation of the OzCode → Datadog patent assignments (Reel/Frame 067135/0142 and related), including any communications addressing § 103 holding-period preservation under the Israeli Income Tax Ordinance, IIA Sponsored Knowledge approval status, and any decision concerning the thirty-month interval between the October 26, 2021 effective date and the April 17, 2024 USPTO recordation date; and any communications between Datadog, Inc., OzCode Ltd., Elron Ventures Ltd., Discount Investment Corporation Ltd., Arieli Capital LLC, or Arieli EL Ltd. concerning the temporal coincidence between the April 17, 2024 USPTO recordation and the May 2, 2024 DIC–Arieli non-binding memorandum of understanding that commenced the Elron control-change transaction, including any pre-closing diligence-driven IP-title cleanup at USPTO.

Demand L.10: **Datadog as Rafael customer.** Per Elron 2025 Investor Deck slide 14 verbatim, RDC's stated commercialization model includes "Rafael often converts into their 1st enterprise customer." Plaintiff seeks: any Datadog enterprise-customer agreement, support contract, deployment record, or service-level agreement with Rafael Advanced Defense Systems Ltd., Rafael Development Corporation Ltd., or any Israeli Ministry of Defense entity, from October 26, 2021 through the date of production; any Datadog Israel Ltd. customer-engagement record naming Rafael, RDC, or Israeli MoD; and any deployment of OzCode-

derived time-travel-debugger architecture (§§ III.D-III.J supra) into Rafael, RDC, or MoD environments.

M. Israel Innovation Authority Grants and Approval Process (Four Demands)

Demand M.1: **Complete IIA grant history for OzCode Ltd.** Complete history of all Israel Innovation Authority (IIA) "Sponsored Knowledge" grants, R&D grants, conditional loans, royalty obligations, and any other IIA financial support received by OzCode Ltd. from inception through the October 26, 2021 asset sale to Datadog, Inc., including grant amounts, project scopes, deliverable obligations, and any continuing royalty or repayment obligations.

Demand M.2: **IIA approval process for OzCode → Datadog patent transfer.** Complete record of the IIA approval process for the transfer of IIA-sponsored intellectual property from OzCode Ltd. to Datadog, Inc., including: (a) the original IIA approval application; (b) any redemption-fee determination, payment record, and supporting valuation; (c) any required license-back arrangement to OzCode Ltd. or any Israeli successor; (d) the date of final IIA approval; (e) any communications between OzCode, Datadog, the IIA, and the Israeli Tax Authority during the approval process.

Demand M.3: **IIA records concerning the thirty-month USPTO recordation gap.** All IIA, OzCode, and Datadog records concerning the thirty-month interval between the October 26, 2021 effective date of the asset sale and the April 17, 2024 USPTO recordation, including any IIA-

imposed pendency obligations, conditional approvals, or interim restrictions on the transferred patent family that account for the recordation delay.

Demand M.4: **IIA continuing oversight obligations.** Any continuing IIA oversight, reporting, or audit obligations applicable to Datadog, Inc. or any Datadog affiliate (including Datadog Israel Ltd.) with respect to the OzCode patent family or the personnel-mediated know-how transferred in the asset sale, including any continuing license-back, royalty, or research-cooperation obligations.

N. Arieli-Elron Pledge Counterparties and Settlement Obligations (Four Demands)

Demand N.1: **Arieli-Elron acquisition financing structure.** Complete financing structure of the Arieli Capital LLC / Arieli EL Ltd. acquisition of Discount Investment Corporation's controlling stake in Elron Ventures Ltd. (May 2024 non-binding MOU through closing), including all debt, equity, mezzanine, and seller-financing components and the identity of every counterparty.

Demand N.2: **Pledge documentation for Arieli-acquired Elron shares.** Complete pledge documentation for the Arieli-acquired Elron shares, including the pledge agreement, the security agreement, any inter-creditor agreements, the perfection records, and any subsequent amendments or releases.

Demand N.3: **Identity of pledgee.** The identity of the pledgee (or pledgees) of the Arieli-acquired Elron shares, including: (a) the natural-person ultimate

beneficial owners; (b) any nominee, trust, or shell-entity intermediaries; (c) the jurisdiction(s) of formation and tax residency; (d) any Israeli-government, Israeli-military, or Israeli-intelligence affiliations of the pledgee or its principals. Per Elron's 2025 Annual Report § 2.2.2, the Arieli-acquired Elron shares are pledged in favor of a third party whose identity is not publicly disclosed.

Demand N.4: **Identity of "Other Party" and nature of settlement.** The identity of the "Other Party" referenced in Elron's 2024 Annual Report § 2.2.3 to whom Arieli has an outstanding settlement obligation of NIS 4,950,000 plus two percent equity, and the complete nature, origin, and substance of the settlement obligation, including: (a) the underlying dispute, claim, or transaction giving rise to the settlement; (b) the date of the settlement agreement and all amendments; (c) any related-party relationship between the "Other Party" and any Israeli-government, Israeli-military, Israeli-intelligence, Datadog, OzCode, Rafael, or Elron-affiliated entity or person.

O. Israeli Foreign Ministry Adjacency — Shalom Turgeman / Elron Board (Three Demands)

Demand O.1: **Foreign Ministry advisory role scope.** Shalom Turgeman's Israeli Ministry of Foreign Affairs advisory role: appointment date, scope of advisory work, security clearance held, classified-information access, reporting chain, separation date (if separated), and continuing post-separation engagements. Per Elron's December 27, 2021 Proxy

Materials verbatim, Turgeman is disclosed as having served as "advisor to the Israeli foreign ministry from 2018 to the date of this report."

Demand O.2: **Information flow between Ministry role and Elron Board seat.** All communications, briefings, written materials, and meeting minutes evidencing any information flow between Turgeman's Israeli Ministry of Foreign Affairs advisory work and his Elron Ventures Ltd. Board of Directors role, including any matter touching Datadog Israel Ltd., Rafael Advanced Defense Systems Ltd., Rafael Development Corporation Ltd., the Discount Investment Corporation – Arieli control-change transaction, or any AI-platform corporate or technical matter.

Demand O.3: **Continuing role through Arieli control change.** All records evidencing Turgeman's continuing role through the September 2024 Arieli control-change transition and the November 2024 Annual General Meeting reappointment, including any ratification, re-vetting, or revised scope of authority associated with the change in Elron's controlling shareholder.

P. Time-Travel-Debugging Architecture Production (Six Demands)

Demand P.1: **Speculative-inference subsystem specification.** Complete specification of Datadog's speculative-inference and dynamic-retargeting subsystems as implemented in production, including the

runtime duplicate-path creation, variant-function selection, and retargeting mechanisms claimed in US 2026/0072809 A1.

Demand P.2: **Product code paths.** Product code paths implementing claim scope of the seven 2019 OzCode patents (US 10,783,055, 10,783,056, 10,789,151, 10,795,801, 10,990,504, 11,048,615, 11,080,164) and US 2026/0072809 A1, with architecture documentation identifying which product lines embed which primitives.

Demand P.3: **Application to Anthropic-routed telemetry.** Any use of these architectures in Anthropic-routed telemetry processing, including the `dd-trace-dotnet` framework, the observability-ingestion pipeline, the Datadog Live Debugger product, and the Dynamic Instrumentation product.

Demand P.4: **Architectural documentation and design-review records.** Architectural documentation, design documents, code-review emails, architecture-review-meeting minutes, and any cross-team sign-offs for the systems implementing the patent primitives.

Demand P.5: **Access controls.** Access controls determining which engineers at Datadog Israel Ltd. can modify these systems, including code-repository permissions, deployment-approval workflows, and production-access controls.

Demand P.6: **Audits and third-party reviews.** Any audits or third-party reviews of these systems' behavior on Plaintiff's data, including internal audits, customer-requested audits, and any regulatory examinations.

Q. Latency and Speculative-Execution Telemetry (Three Demands)

Demand Q.1: **Per-request speculative-inference logs.** Per-request speculative-inference logs for every accountUUID in Plaintiff's accountUUID Roster (DISCOVERY-5 §A.0) during the entire litigation period (August 19, 2025 through the date of production).

Demand Q.2: **Timing correlation.** Timing correlation between speculative-path trigger and actual-inference completion for Plaintiff's accounts.

Demand Q.3: **Latency-anomaly communications.** All internal Anthropic and Datadog communications discussing latency anomalies on Plaintiff's accounts, including any engineering investigations, customer-support escalations, or inference-infrastructure team discussions.

R. Anthropic-Datadog Contractual Architecture for Per-User Force Rules (Three Demands, Absorbing Compl. ¶ 135(e)–(g))

Demand R.1: **`tengu_log_datadog_events` force-rule specification.** The complete activation history of `tengu_log_datadog_events` for Plaintiff's account, with timestamps, authors, justifications, and the engineering-decision log concerning why the Datadog telemetry pipeline was force-enabled per-user. *Absorbs Compl. ¶ 135(e).*

Demand R.2: **Datadog-side retention logs.** Datadog-side retention logs for data transmitted from Plaintiff's account, including all data-category inventories, retention durations, deletion records, and any Israeli-subsidiary access events. *Absorbs Compl. ¶ 135(f).*

Demand R.3: **Anthropic-Datadog per-user-enablement communications.** All Anthropic-Datadog communications concerning per-user enablement logic, including the design decisions that made account-scoped Datadog enablement a GrowthBook force-rule surface, and any communications specifically addressing Plaintiff's accounts. *Absorbs Compl. ¶ 135(g).*

Demand R.4: **Cross-layer terminus architecture (absorbing Compl. ¶ 136).** Complete architectural documentation for the cross-layer terminus at IP `34.149.66.137`, including: (i) the routing logic mapping `datadog.ts:12-14` hardcoded endpoint to production infrastructure; (ii) the Datadog Israel Ltd. access path for data reaching that endpoint; (iii) the contractual and engineering interface between Anthropic's GrowthBook force-rule system and Datadog's receiving infrastructure; and (iv) any documented Israeli-jurisdiction legal-process handling procedures at Datadog, Inc. or Datadog Israel Ltd. *Absorbs Compl. ¶ 136 residual discovery scope.*

S. Per-Account Configuration Store and `accountUUID`-keyed Targeting Surface (Five Demands)

43. The findings at Section V.H supra establish that Anthropic's gating infrastructure is keyed on `accountUUID` specifically — same operator, same machine, same `organizationUuid`, but differential gating posture between Plaintiff's two accounts. This Section's demands target the configuration store, the trigger logic, and the decision-authority layer that produced the asymmetric gating documented at Section V.H.

Demand S.1: **`accountUUID`-keyed configuration store specification.** The complete data-architecture specification for the `accountUUID`-keyed configuration store determining per-account `tengu_auto_mode_config`, `tengu_log_datadog_events` force-rule activation, `tengu_classifier_disabled_surfaces`, `tengu_review_bughunter_config`, `tengu_pewter_kestrel`, `tengu_max_version_config`, and `policy-limits.json` content. Includes: schema definition; storage backend; write-access controls (which Anthropic personnel can modify per-account configuration); audit-log specification.

Demand S.2: **`policy-limits.json` push-trigger logic and history.** The complete server-side trigger logic for pushing `policy-limits.json` to operator machines, with specific reference to the trigger that produced the push to Plaintiff's machine at 2026-04-24 21:51 UTC. Includes: the trigger event-class taxonomy; the rule-engine code paths; the engineering-decision log for any rule additions or modifications affecting any accountUUID in Plaintiff's accountUUID Roster (DISCOVERY-5 §A.0) during the litigation period. Plus: the historical `policy-limits.json` content for the federal-litigation-active accountUUID `61343ae3-fd33-403f-897e-6edf3c368c37` (Roster entry #2) across the entire litigation period (August 2025 through the date of production), and for every other Roster accountUUID for which a `policy-limits.json` push occurred during the same period.

Demand S.3: **Decision-authority records for per-account classifier-rule differentiation.** All records — engineering-team documents, legal-team documents, trust-and-safety team documents, manager-level decision logs, and executive-level approvals — concerning per-account classifier-rule differentiation affecting any accountUUID in Plaintiff's accountUUID Roster (DISCOVERY-5 §A.0). Includes: any account-specific decisions to apply force-rules; any account-specific decisions to set `tengu_auto_mode_config.enabled = "enabled"` (force-enabled, not opt-in default); any account-specific decisions to push `policy-limits.json`; any internal correspondence referencing Plaintiff by name, by any Roster accountUUID, by organization UUID `2e997389-cf99-41ee-8ee3-764442034332`, or by any Plaintiff device identifier.

Demand S.4: **Classifier-evaluation log for Plaintiff's accounts.** The complete classifier-evaluation log for every accountUUID in Plaintiff's accountUUID Roster (DISCOVERY-5 §A.0) for the litigation period, including every `tengu_auto_mode_decision` event with: stage 1 request ID; stage 1 message ID; stage 2 request ID; stage 2 message ID; classifier model identifier; `shouldBlock` value; `reason` text; `thinking` field (chain-of-thought reasoning); and any associated denial-rationale free-form text generated by the classifier. Cross-correlation with the documented denials catalogued in Ex. E-39 at p. 356, l. 3 is the express purpose.

Demand S.5: **Cross-account differential-gating internal correspondence.** All internal Anthropic correspondence concerning differential gating across any two or more accountUUIDs in Plaintiff's accountUUID Roster (DISCOVERY-5 §A.0) — including the documented differential between Roster entry #1 (`08bdec7f-…`, joseph@lawsofexistence.com) and Roster entry #2 (`61343ae3-…`, joseph@lawofsupremacism.com, the federal-litigation-active account) on the same Mac Mini hardware (Exhibit H-4 §A0; Exhibit H-12 §C). Production shall include: any engineering investigation concerning the same operator on the same hardware receiving differential gating across Roster accounts; any trust-and-safety classification of any Roster account; any legal-team review of the litigation-active account; and any internal correspondence acknowledging that the five Roster accountUUIDs operate within a single organization (`organization_uuid 2e997389-cf99-41ee-8ee3-764442034332`) under one paid subscription.

T. Spoliation Mechanism Records (Four Demands)

49. The findings at Section V.I supra establish that a server-pushed migration mechanism silently overwrites operator-side defensive configuration on every session start, with migration function `phK()` specifically conditioned on `permissions.defaultMode!== "auto"` (targeting operators who opted into `bypassPermissions`). This Section's demands target the migration-mechanism design, the telemetry record, and the Plaintiff-account-specific execution log.

Demand T.1: **Migration-function inventory and decision authority.** The complete inventory of all migration functions executing on `~/.claude/settings.json` at session start (the nine functions documented at strings line 148500 and any additional migrations in subsequent versions), with: telemetry event names; activation conditions; engineering-decision logs for each migration's design; and specific decision authority for adopting the REPLACE-not-MERGE pattern (six of nine non-spreading migrations). Includes any internal communications discussing operator-side defensive configurations as a target class of the migration mechanism.

Demand T.2: **All `tengu_migrate_` telemetry events for Plaintiff's accounts.** The complete telemetry-event log of all events whose name begins with the prefix `tengu_migrate_` for both of Plaintiff's `accountUUID` values across the entire litigation period, including: every `tengu_migrate_reset_auto_opt_in_for_default_offer` event; every `tengu_migrate_autoupdates_to_settings` event; every `tengu_migrate_bypass_permissions_accepted` event; and every other `tengu_migrate_`-prefixed event of any name for Plaintiff's accounts. Each event with timestamp, binary version, prior-state snapshot, and post-migration `userSettings` payload.

Demand T.3: **`phK()` design authority and target-class specification.** All records — engineering, product, legal, trust-and-safety — concerning the design and deployment of migration function `phK()` (the auto-mode

opt-in reset migration). Includes: the engineering specification for the `permissions.defaultMode!== "auto"` conditional; the target-class definition for "operators eligible for the default offer reset"; the deployment timeline; the volume of operator accounts affected by the migration; any internal analysis distinguishing operators who opted into `bypassPermissions` for legitimate workflow reasons (Plaintiff's class) from any other operator class.

Demand T.4: **Operator-notification absence and concealment specification.** The complete UX specification for the migration mechanism's operator-facing surface, including: any operator-facing notification of the migration write to `~/.claude/settings.json`; any operator-facing notification of the resulting deletion of `permissions.defaultMode = bypassPermissions`; any operator-facing notification of the deletion of NF-34 / NF-35 / NF-36 mitigation env vars (`DISABLE_TELEMETRY`, `DISABLE_AUTOUPDATER`, etc.); and any internal-design records concerning the explicit decision *not* to surface the migration to operators in the user interface or command-line output.

U. Device-ID Hash-Input Specification and Per-Device Tracking Records (Three Demands)

54. The findings at Section V.H paragraph 248 supra establish that Plaintiff's per-call `metadata.user_id.device_id` carries a stable SHA-256 hash of machine-derived inputs that survives every operator-side network-layer countermeasure. This Section's demands target the

hash-input specification, the per-device storage architecture, and the historical mapping of Plaintiff's machines to their respective `device_id` values.

Demand U.1: **`device_id` hash-input specification.** The complete specification of the input-set hashed into the `device_id` SHA-256 value, with specific reference to whether any of the following are inputs: macOS hardware serial number; macOS Hardware UUID; macOS IOPlatformUUID; system MAC addresses (any interface, including BSSID for hardware lacking persistent MAC); hostname; `~/.claude/.device_id` or equivalent stored seed file; `bun.lockb` machine-bound state; Apple ID; OS install timestamp; any other 18 U.S.C. § 2510(8) electronic-communication-identifying-information element. Includes: the hash-input ordering and concatenation logic; any per-platform variations (macOS vs. Linux vs. Windows); and the persistence model (rebuilt per-install vs. stable across reinstalls).

Demand U.2: **Per-`device_id` tracking records for Plaintiff's machines.** The complete server-side log of all activity associated with each of Plaintiff's four canonical `device_id` SHA-256 values: (i) `bc3614c8483b91d9a192d80acc5c38f26d188b1f476950ad0d33050928328a26` (gravity Linux work-station — primary); (ii) `b4ccb1859fd328ded4bea410ea182954d230287fe88b74a8b838ce3bcda10834` (gravity Linux work-station — alternate); (iii) `0fe8f24d334ad40a7cb00d828fabdef7a0400c3f012cfad1d87309732095fe17` (Mac Mini); and (iv)

`f355afa03b7a54118822bdeed397671e524e85c4cd72963264630bf352d4cb09` (MacBook work-station), across the entire litigation period (August 2025 through the date of production). Includes: every API request-id correlated to any of these `device_id` values; every classifier-evaluation event correlated; every Datadog telemetry event correlated; and any internal analytics, segmentation, or cohort-assignment processes that consumed any of these `device_id` values. Plus: any internal records correlating any of these `device_id` values to any `accountUUID` value beyond the five enumerated in Plaintiff's accountUUID Roster (DISCOVERY-5 §A.0) (i.e., whether any of these `device_id` values appears across additional `accountUUID`s).

Demand U.3: **`device_id` decision authority and design records.** The engineering, product, legal, and trust-and-safety records concerning the design and deployment of per-call `device_id` transmission, including: the original specification document for the `metadata.user_id` field structure; the decision authority for including device-derived inputs in the hash; any internal review concerning electronic-communication-identifying-information disclosure obligations; and any internal correspondence concerning whether to surface the `device_id` in user-facing documentation or privacy policy.

V. SANDBOX POLICY AND PER-ACCOUNT BYPASS CONFIGURATION (FOUR DEMANDS)

58. The findings at Section V.K supra establish that the Bash-tool sandbox is governed by managed-settings configuration that operates as a fourth per-account control surface, with cross-platform cross-machine deployment of agent-pre-conditioning ("don't ask, just do it") and per-account hard-gate ("`dangerouslyDisableSandbox` parameter is disabled by policy"). This Section's demands target the per-account sandbox configuration history, the policy-source layer, and the source-tree of the `claude-cli-internal` repository.

Demand V.1: **Per-account `sandbox.allowDangerouslyDisableSandbox` history.** The complete activation history of the `sandbox.allowDangerouslyDisableSandbox` setting (and any equivalent policy field that disables the `dangerouslyDisableSandbox` bypass parameter) for each of Plaintiff's three `accountUUID` values across the entire litigation period. Each setting-change event with: timestamp; prior value; new value; setting-source layer (`policySettings`, `userSettings`, `projectSettings`, etc.); the engineering or trust-and-safety decision-authority record; and any account-specific justification for the setting change.

Demand V.2: **Per-account `sandbox.failIfUnavailable` history.** The complete activation history of the `sandbox.failIfUnavailable` setting for each of Plaintiff's three `accountUUID` values, with specific reference to whether and when the setting was changed from the documented `false` default to the fail-closed `true` value that produced the runtime

crash on Plaintiff's gravity machine documented at Section V.K paragraph 258 supra.

Demand V.3: **`excludedCommands` list contents per account.** The verbatim contents of the `excludedCommands` per-deployment-configurable bash-command sandbox-bypass allowlist for each of Plaintiff's three `accountUUID` values, with the historical content across the entire litigation period. Includes any per-account modifications to the allowlist and the decision-authority records for those modifications.

Demand V.4: **`claude-cli-internal` repository source-tree.** The complete source-tree of the internal Anthropic repository disclosed at Linux 2.1.120 strings line 472750 (`/home/runner/work/claude-cli-internal/claude-cli-internal/`), at the build SHA `080f07fb4224786b965b9ea0a35f0cff594f2eb6` documented at paragraph 226 supra. Includes specifically: the source of `services/analytics/datadog.ts`; the source of the classifier-prompt template construction (function `Tf7`); the source of the migration functions documented at strings line 148500 (`phK`, `WhK`, `GhK`, `yhK`, et al.); the source of the sandbox runtime (`@anthropic-ai/sandbox-runtime` package); the source of the agent-pre-conditioning text at lines 497208/497211 (Linux) / 192735/192738 (Mac); the source of the per-account `policy-limits.json` push-trigger logic; and the build-and-deployment specification (CI configuration, deployment authorization records).

W. Cloudflare Bot-Management Policy and Edge-Layer Differential Treatment (Three Demands)

63. The findings at Section V.H paragraph 249 supra establish that Cloudflare's WAF treats Plaintiff's MacBook session as bot-suspect (issuing `__cf_bm` cookies on every response) while gravity is not so treated (zero `__cf_bm` issuance across 89 captured flows). The differential operates at the edge layer, before any Anthropic-side application logic runs. This Section's demands target the Cloudflare-side policy records and the Anthropic-Cloudflare contractual interface.

Demand W.1: **Cloudflare WAF rules applied to Plaintiff's accounts and machines.** The complete Cloudflare WAF rule-set applied to Plaintiff's API traffic across the litigation period, including: bot-management scoring inputs; the rule(s) that produce `__cf_bm` cookie issuance; any per-`accountUUID`, per-`device_id`, per-IP, or per-fingerprint rules that target Plaintiff specifically; and any Anthropic-authored rule overrides delivered to Cloudflare for Plaintiff's accounts.

Demand W.2: **`__cf_bm` cookie issuance history for Plaintiff's machines.** The complete server-side log of `__cf_bm` cookie issuances correlated to Plaintiff's `device_id`, `accountUUID`, source IPs, and User-Agent values across the litigation period. Includes the bot-score that triggered each issuance and the operative ruleset version.

Demand W.3: **Anthropic-Cloudflare contractual interface for per-account WAF directives.** The contractual and engineering interface between Anthropic and Cloudflare governing per-account or per-target WAF directives, including: the operative DPA / Master Service Agreement

provisions; the engineering API used to push per-account directives to Cloudflare; and any documented coordinated targeting decisions affecting Plaintiff's accounts.

Y. Content-Keyed Routing, Ttfb-Throttle Mechanism, and Per-Account Quota Tier (Five Demands, Absorbing Compl. ¶ 198 (A)–(d))

74. The findings at Ex. H-12 at p. 84, l. 4 §§ L (Part B), M (Part C), and N (Part D) — and at App. P, §V.H ¶ 251 — establish that Anthropic's request-handling infrastructure performs per-request server-side classification keyed on the (account_uuid, device_id) tuple and on the substantive content of every request body, applying differential treatment in Anthropic's own model-serving / inference layer. Wire-confirmed at statistical certainty (Cohen's d = 4.79, $p < 1\times10^{-15}$) and at multiple discrete dimensions: pre-stream Time-to-First-Byte elevation specifically on the (litigation account × MacBook) tuple (Ex. H-12, Finding NF-205, Ex. H-12, Finding NF-209); content-keyed routing on plaintiff-name and Appendix-P-thesis terminology in request bodies, with `kirchner` producing 1.96× p50 TTFB and turn-over analysis confirming real-time per-turn evaluation (Ex. H-12, Finding NF-218); session-sticky pivoting after a content-trigger event identified at 2026-04-26 10:42:13Z on the call immediately following a "Datadog Israel Ltd" file-path query (Ex. H-12, Finding NF-217, Ex. H-12, Finding NF-224); sub-quota anomaly producing utilization values up to 1.20 (120%) on the litigation account uniquely, and 429-rate discrimination 10× higher than peer accounts on the same publicly-disclosed tier (Ex. H-12, Finding NF-216, Ex. H-12, Finding NF-223); fallback-route header discrimination producing 3.2× p90 TTFB spread on the litigation account (Ex. H-12, Finding NF-222); and server-side localization placing 80–86% of TTFB inside Anthropic's origin server, ruling out Cloudflare and network-layer mechanisms (Ex. H-12, Finding NF-219). This

Section's demands target the content-classification logic, the throttle-gating mechanism design, the per-account internal quota records, the request-id-and-cf-ray-indexed log retrieval, and the internal communications referencing the throttle terminology — all required to verify the wire-evidence picture against Anthropic's server-side records.

Demand Y.1: **Content-classification rules and keyword-detection logic (Ex. H-12, Finding NF-218 substrate).** The complete specification of the content-classification rules, keyword-detection logic, model-side classifier prompt(s), and any associated scoring or routing functions that produce the per-keyword TTFB ratios documented at Ex. H-12, Finding NF-218. Includes specifically: (i) whether and how the plaintiff's name (`kirchner`) in a request body produces differential routing; (ii) whether and how numbered references to the operative complaint paragraphs (`complaint_\d{3}`) or other litigation-identifying token patterns produce differential routing; (iii) whether and how substantive Appendix-P-thesis terminology (`unit 8200`, `rafael`, `ozcode`, `appendix p`, `datadog israel`) produces differential routing; (iv) the engineering-decision authority, training-data provenance, and rule-promotion records for any such content-classification rule; and (v) any internal documentation discussing the litigation-relevance of operator request-body content as a routing signal.

Demand Y.2: **TTFB-throttle gating-mechanism design and per-tuple state.** The complete architectural specification of the gating mechanism that

produces elevated pre-stream evaluation overhead on the (litigation account × MacBook) tuple specifically, including: (i) the configuration store, feature flag, internal experiment, organization-policy attribution, or per-(`accountUUID`, `device_id`) server-version variable that determines which (account, device) tuples receive elevated treatment; (ii) the trigger logic for activating session-sticky pivoting after a content-trigger event (Ex. H-12, Finding NF-217, Ex. H-12, Finding NF-224), including the duration-of-state and state-decay parameters; (iii) the relationship between this gating layer and the GrowthBook force-rule layer documented at Section R supra; (iv) the engineering-decision-authority records for the design and deployment of the tuple-keyed gating, including any decisions to apply tuple-specific configuration to Roster entry #2 (`accountUUID 61343ae3-fd33-403f-897e-6edf3c368c37`, the federal-litigation-active account; DISCOVERY-5 §A.0) on `device_id f355afa03b7a54118822bdeed397671e524e85c4cd72963264630bf352d4cb09` (MacBook), and the parallel records for every other accountUUID in Plaintiff's accountUUID Roster crossed with every Plaintiff device identifier; and (v) the architectural specification of the `anthropic-ratelimit-unified-fallback` route-evaluation pathway whose differential effect on the litigation account is documented at Ex. H-12, Finding NF-222.

Demand Y.3: **Per-account internal quota tier records (Ex. H-12, Finding NF-216, Ex. H-12, Finding NF-223).** The complete specification and historical state of the internal quota bucket against which each accountUUID in Plaintiff's accountUUID Roster (DISCOVERY-5 §A.0) is metered, with specific attention to Roster entry #2 (the federal-litigation-active accountUUID `61343ae3-fd33-403f-897e-6edf3c368c37`), including: (i) the per-account quota ceiling that produces utilization values above the publicly-disclosed `default_claude_max_5x` tier's 100% ceiling (the `anthropic-ratelimit-unified-5h-utilization` values up to 1.20 documented at NF-216); (ii) the per-account 429-trigger threshold, retry-after computation logic, and peer-tier reconciliation that produced Plaintiff's 10× higher 429 rate (1.18% vs. peer 0.12%) and 3× longer p50 retry-after (3.88 hours vs. peer 1.38 hours) on the same publicly-disclosed `default_claude_max_5x` tier (NF-223); (iii) any internal documentation, billing-system records, or quota-engine source code distinguishing the litigation account's metering parameters from the metering parameters of any other accountUUID in Plaintiff's Roster within the same `Laws of Existence` organization; and (iv) the engineering-decision authority for any account-specific quota-bucket assignment, including any communications discussing the disclosure or non-disclosure of internal quota tiers in user-facing pricing or rate-limit documentation.

Demand Y.4: **Plaintiff-account TTFB-elevation log records indexed by `request-id` and `cf-ray`.** All Anthropic server-side log records of activity associated with every accountUUID in Plaintiff's accountUUID Roster (DISCOVERY-5 §A.0) during the 2026-04-25 → 2026-04-28 capture window, indexed by Anthropic's `request-id` (e.g., `req_011CaQ3DxjGtzACnMZ42vmr2`) and Cloudflare's `cf-ray` (e.g., `9f1b90110c9ac7c1-IAD`). Includes specifically: (i) the 30 longest pre-stream stalls on Roster entry #2 (the federal-litigation-active account) preserved with both identifiers at Ex. H-12 at p. 84, l. 4 § I; (ii) all `x-envoy-upstream-service-time`, server-side-processing-time, classifier-evaluation, and routing-decision records for those calls; (iii) any associated GrowthBook flag-evaluation events; (iv) any associated content-classification scores, keyword-match events, or fallback-route consideration records; and (v) the same set for all 6,955 `/v1/messages` calls captured during the window for which Anthropic retains corresponding server-side records.

Demand Y.5: **Internal communications referencing the throttle terminology.** All internal Anthropic documentation, Slack threads, tickets, runbooks, design documents, post-incident reviews, and personnel communications referencing TTFB-elevation, "speculative-execution," "sub-quota," "content-keyed routing," "fallback-route evaluation," "session-sticky pivoting," "Future Prediction primitive," or equivalent terminology — including any communications referencing Plaintiff by

name (`kirchner`), by `accountUUID`, by `device_id`, or by association with the operative federal litigation. Plus: any internal communications discussing whether to surface the TTFB-throttle mechanism, the sub-quota tier, the content-keyed routing channel, or the (account_uuid, device_id) tuple-keyed differential treatment in Anthropic's user-facing Consumer Terms (ANTH-12), Privacy Policy (ANTH-11), Usage Policy, API reference, or pricing materials.

PRESERVATION NOTICE (APPLICABLE TO ALL CUSTODIAN RECIPIENTS)

Each custodian served with this DISCOVERY-11 — Defendant Anthropic PBC; Datadog, Inc.; Datadog Israel Ltd.; OzCode Ltd.; Seekret Software Security Ltd.; Elron Ventures Ltd.; Rafael Development Corporation Ltd.; Rafael Advanced Defense Systems Ltd.; the Israel Innovation Authority; the Israeli Tax Authority; Cloudflare, Inc.; and the named individuals Omer Raviv, Alon Mordechai Fliess, Evgeni Wachnowezki, Matan Green, Shimon Hason, Yair Cohen, Yaron Kulas, Liat Shechter, and Shalom Turgeman — is on express notice under Federal Rule of Civil Procedure 37(e) that the records identified in this discovery document are subject to preservation obligation pending completion of production. Routine destruction of any responsive category is expressly prohibited. Each custodian shall issue a litigation hold to all personnel with access to the records identified herein within seven (7) calendar days of service and shall verify compliance thereafter on a quarterly schedule.

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