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-6: DEFENDANT APPLE INC.

INTRODUCTION

This document replaces in its entirety the January 2026 draft of DISCOVERY-6. The rebuild is driven by the following material changes to the evidentiary record:

1. **The F-series exhibit expansion (F-1 through F-29).** Plaintiff's forensic analysis of Apple's Xcode Intelligence, Apple Intelligence, IDELanguageModelKit, ExternalModelService, SmootML analytics, Biome activity tracking, iCloud synchronization, Messages container retention, and certificate-pinning infrastructure is now documented in 29 F-series exhibits with source-code-level and packet-capture-level specificity. F-27/28/29 — Messages container

litigation retention, Messages container verification extraction, and source-code cross-verification — were added during Q1 2026 and were not available for the January draft.

2. **The March 31, 2026 Anthropic source code release** (Ex. E-32 at p. 235, l. 3). The Leaked Source independently verifies cross-defendant coordination patterns between Apple and Anthropic at the source-code level, including the Apple Floodgate proxy integration (Ex. F-4 at p. 22, l. 2) and IDELanguageModelKit routing to external providers (Ex. F-6 at p. 33, l. 2).

3. **The F-29 source-code cross-verification exhibit** (Ex. F-29 at p. 133, l. 3) establishes that Plaintiff's prior binary-level forensic findings regarding Xcode Intelligence, IDELanguageModelKit, and ExternalModelService are confirmed at the source-code level, transforming every verified finding from "Plaintiff's forensic analysis claims X" to "Apple's own source-code confirms X."

The pre-leak draft's organizing theory — "Xcode Intelligence hidden instructions → iCloud synchronization → file path exposure → coordinated conduct → XProtect detection" — is preserved in substance, but the evidentiary predicate has thickened materially. The rebuild is organized by **evidentiary architecture**: each Phase corresponds to a concrete mechanism documented in one or more F-series exhibits; each Category targets specific findings.

DEFINITIONS AND CONVENTIONS

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

- **"Xcode Intelligence"** means the Apple IDE-integrated AI-assistance features available in Xcode during the relevant period, including but not limited to the "Coding Assistant," "Predictive Code Completion," and any feature routed through `IDELanguageModelKit` or `ExternalModelService`.
- **"Apple Intelligence"** means Apple's operating-system-integrated AI platform as deployed on macOS and iOS during the relevant period, including but not limited to Writing Tools, Image Playground, and any feature that routes to a third-party model provider.

- **"IDELanguageModelKit"** means the framework and binaries by the name `IDELanguageModelKit`, including `.framework`, `.dylib`, and `.bundle` payloads, as documented at Ex. F-6 at p. 33, l. 2 and Ex. F-22 at p. 94, l. 2.

- **"ExternalModelService"** means the macOS system service of that name, including its daemon binary and associated configuration, as documented at Ex. F-16 at p. 72, l. 2.

- **"Floodgate"** means the Apple-operated proxy infrastructure identified at Ex. F-4 at p. 22, l. 2 through which AI traffic is routed during the relevant period.

- **"Biome"** means the macOS/iOS Core Biome / knowledge-graph activity-tracking database as documented at Ex. F-9 at p. 44, l. 2 and the associated crash-log pipeline at Ex. F-20 at p. 88, l. 2.

- **"SmootML"** means the Apple analytics subsystem by that name, as documented at Ex. F-12 at p. 55, l. 2 and Ex. F-23 at p. 101, l. 2.

- **"Plaintiff's Apple account"** means every Apple ID ever associated with Plaintiff — including (without limitation) every Apple ID bound to any email address on the domains `lawsofexistence.com` or `lawofsupremacism.com` (both of which are owned and operated by Plaintiff and the Laws of Existence LLC organization, including without limitation `legal@lawsofexistence.com`, `partnership@lawofsupremacism.com`, `info@lawofsupremacism.com`, and `contact@lawofsupremacism.com`), and every Apple ID bearing Plaintiff's name "Joseph Kirchner" — together with any associated iCloud account, Messages account, FaceTime registration, Apple Developer account, and every registered hardware device.

- **"Plaintiff's devices"** means every Apple hardware device associated with Plaintiff's Apple account, including the MacBook Pro on which the forensic captures underlying the F-series exhibits were made.

- **"Relevant period"** means January 1, 2025 through the date of production, unless otherwise specified.

Production format: Native-format files wherever feasible (framework binaries, `.plist` files, `.sqlite` / `.db` snapshots, packet captures, system logs). Redaction for unrelated customer data is permitted pursuant to a mutually negotiated protective order; redactions must be accompanied by a redaction log.

PHASE A: APPLE INTELLIGENCE MULTI-PROVIDER AI ROUTING (21 DAYS)

Counts developed by this Phase: Compl., Count X (Consumer Protection / Deceptive Trade Practices), Compl., Count XII (ECPA, 18 U.S.C. § 2511), Compl., Count XV (App Store Misrepresentation), Compl., Count V (42 U.S.C. § 1985 Conspiracy).

CATEGORY AA: IDELANGUAGEMODELKIT FRAMEWORK

REQUEST NO. 1: Complete source code, header files, binary symbol tables, and documentation for `IDELanguageModelKit.framework` in every version deployed during the relevant period, including:

(a) The complete public and private header files

(b) The complete public and internal class, protocol, and function inventory

(c) Every model-provider adapter included in the framework (Apple internal, OpenAI, Anthropic, any additional)

(d) Every configuration file, plist, and resource bundle contained in the framework

(e) Every commit, pull request, and code-review record for the framework's development

Evidentiary predicate: Ex. F-6 at p. 33, l. 2 documents the framework's multi-provider AI-integration architecture.

REQUEST NO. 2: All documents describing IDELanguageModelKit's routing logic, including:

(a) The decision-making rules that select one provider over another for a given user request

(b) The flags, configuration settings, or runtime conditions that influence routing

(c) Any per-user, per-account, or per-device targeting rules

(d) Any A/B-test or experiment result regarding routing decisions

REQUEST NO. 3: Complete documentation of the safety and content-filtering subsystem operative within IDELanguageModelKit during the relevant period, including:

(a) The source code for the safety classifier(s)

(b) The training data and ground-truth corpus used to train or tune each classifier

(c) Every category, rule, or signal used to classify content

(d) Any differential filtering applied based on user, account, or device identity

Evidentiary predicate: Ex. F-22 at p. 94, l. 2 documents the safety-and-content-filtering architecture.

CATEGORY AB: EXTERNALMODELSERVICE PROCESS

REQUEST NO. 4: Complete source code, launchd configuration, and operational documentation for `ExternalModelService` in every version deployed during the relevant period, including:

(a) The full binary inventory (daemon, helpers, helper tools)

(b) The launchd plist(s) defining the service

(c) The XPC or Mach interface(s) through which clients invoke the service

(d) The service's network configuration (allowed destinations, cert-pinning configuration, proxy configuration)

Evidentiary predicate: Ex. F-16 at p. 72, l. 2 documents the process's AI-request-routing function.

REQUEST NO. 5: All records of `ExternalModelService` invocations on Plaintiff's devices during the relevant period, produced per-invocation with: (a) the originating client; (b) the prompt content; (c) the resolved

destination provider; (d) the response content; (e) the retention of each of the foregoing on Plaintiff's device and on Apple backend systems.

REQUEST NO. 6: All documents regarding the design of `ExternalModelService` as a privileged system service, including:

(a) The rationale for making model invocation a system service rather than an in-process library
(b) Any discussion of the privilege-escalation implications
(c) Any legal or privacy review of the transmission-off-device consequence

CATEGORY AC: SAFETY / CONTENT-FILTERING DIFFERENTIAL

REQUEST NO. 7: All documents regarding differential safety or content-filtering applied to Xcode Intelligence or Apple Intelligence users based on:

(a) User identity (Apple ID, device UDID, IP address)
(b) Account tier (iCloud, iCloud+, Apple Developer, Enterprise)
(c) Device profile (configuration profile, MDM enrollment, Developer-mode enrollment)
(d) Geographic region or locale

REQUEST NO. 8: All A/B-test results, experiment records, or research memoranda regarding the effect of safety filtering on model capability or user experience, including any documents acknowledging a capability differential attributable to the filtering layer.

PHASE B: XCODE INTELLIGENCE TRANSMISSION (21 DAYS)

Counts developed by this Phase: Compl., Count XII (ECPA, 18 U.S.C. § 2511), Compl., Count XIII (CFAA, 18 U.S.C. § 1030), Compl., Count IX (Breach of Contract), Compl., Count XIV (CCPA / State Privacy).

CATEGORY BA: DEFINITIVE SOURCE-CODE TRANSMISSION PROOF

REQUEST NO. 9: Complete documentation of Xcode Intelligence's transmission of customer source code to any destination (internal Apple, OpenAI, Anthropic, or other third-party provider) during the relevant period, including:

(a) The complete set of API endpoints that receive source-code content
(b) The payload schema for each endpoint
(c) The scope of source-code transmission (selection only, file only, project only, workspace only, with or without surrounding files)
(d) The retention policy at each destination
(e) The downstream consumer of each transmission

Evidentiary predicate: Ex. F-17 at p. 76, l. 2 documents the packet-capture-level proof of source-code transmission.

REQUEST NO. 10: All records of source-code transmission from Plaintiff's Xcode sessions during the relevant period, produced per-transmission with: (a) the source file path and line range transmitted; (b) the destination endpoint; (c) the identity of the ultimate consumer (Apple-internal model, third-party model); (d) the retention of the transmitted content.

REQUEST NO. 11: All documents regarding Apple's internal analysis of whether Xcode Intelligence's source-code transmission complies with:

(a) Developer Program License Agreement restrictions on use of customer code
(b) Apple's own privacy policies and App Store representations
(c) State privacy law (CCPA, CPRA, BIPA, or other)
(d) Federal privacy and wiretap law

CATEGORY BB: PER-SESSION NETWORK TRAFFIC

REQUEST NO. 12: Complete per-session network-traffic documentation for Xcode Intelligence during the relevant period, including:

(a) The full inventory of endpoints contacted per-session
(b) The byte-count distribution per endpoint
(c) The connection-lifetime distribution
(d) Any differential behavior based on user, project size, or device configuration

Evidentiary predicate: Ex. F-15 at p. 67, l. 2 documents the per-session network-traffic architecture.

REQUEST NO. 13: Complete packet-capture records from Apple's side for every Xcode Intelligence session attributable to Plaintiff's Apple account during the relevant period.

REQUEST NO. 14: All documents describing the relationship between per-session traffic and billing, analytics, or training pipelines, including:

(a) Any documents identifying the purpose of each endpoint contacted
(b) Any documents acknowledging that the endpoint list is not disclosed to users
(c) Any customer-facing disclosure (or absence thereof) of the per-session connection count

CATEGORY BC: OAUTH TOKEN EXPOSURE

REQUEST NO. 15: Complete documentation of OAuth token handling in Xcode Intelligence during the relevant period, including:

(a) The OAuth clients authorized for Xcode Intelligence integration
(b) The scope requested by each client
(c) The storage location and protection regime for obtained tokens
(d) The rotation and revocation infrastructure for each token class

Evidentiary predicate: Ex. F-18 at p. 81, l. 2 documents OAuth-token exposure in the Xcode cache.

REQUEST NO. 16: All documents regarding the decision to cache OAuth tokens in user-readable locations within the Xcode cache, including:

(a) The authorization for the caching design
(b) Any security or privacy review acknowledging the exposure
(c) Any response to Plaintiff's forensic finding regarding the exposure
(d) Any patch, rotation, or remediation deployed after the forensic finding was communicated to Apple

CATEGORY BD: CODING ASSISTANT METADATA PLIST

REQUEST NO. 17: Complete documentation of the Xcode Coding Assistant metadata plist file(s) and their downstream consumers, including:

(a) The complete schema of each plist file written by the Coding Assistant
(b) The locations on disk where each is written
(c) The access-control regime protecting each
(d) Every downstream consumer (local process, backend pipeline, third-party SDK)

Evidentiary predicate: Ex. F-21 at p. 91, l. 2 documents the metadata-plist file analysis.

REQUEST NO. 18: All Coding Assistant metadata plist files written on Plaintiff's devices during the relevant period, produced as native files with timestamps.

PHASE C: CERTIFICATE PINNING AND BYPASS (21 DAYS)

Counts developed by this Phase: Compl., Count XII (ECPA, 18 U.S.C. § 2511), Compl., Count X (Consumer Protection / Deceptive Trade Practices).

CATEGORY CA: DELIBERATE OPACITY DESIGN

REQUEST NO. 19: Complete documentation of Apple's certificate-pinning design for Xcode Intelligence, Apple Intelligence, and Floodgate-routed traffic during the relevant period, including:

(a) The list of endpoints subject to pinning
(b) The pinning implementation (static pin list, CRL/OCSP enforcement, Certificate Transparency enforcement)
(c) The documentation of the pinning to users and to researchers
(d) Any design document describing the decision to adopt pinning as an opacity mechanism rather than purely as a security mechanism

Evidentiary predicate: Ex. F-13 at p. 59, l. 2 documents deliberate-opacity design.

REQUEST NO. 20: All internal communications referencing the effect of certificate pinning on:

(a) Researcher forensic analysis
(b) Enterprise monitoring tools (including MDM-distributed security proxies)
(c) Network-level auditing by device owners
(d) Regulatory auditing under CCPA or other privacy law

REQUEST NO. 21: All documents regarding the relationship between certificate pinning and App Store Privacy Nutrition Label filings, including any analysis acknowledging that pinning forecloses user verification of Privacy Nutrition Label claims.

CATEGORY CB: BYPASS FORENSIC METHODOLOGY

REQUEST NO. 22: All internal responses, communications, or remediation plans developed after the forensic methodology documented at Ex. F-10 at p. 48, l. 2 became known to Apple, including:

(a) Any patch or counter-measure deployed in response
(b) Any communication with law enforcement, computer-emergency-response, or security-research communities
(c) Any public statement characterizing the methodology

REQUEST NO. 23: All documents regarding Apple's policy for responding to researcher-disclosed methods of bypassing Apple's anti-forensic infrastructure, including the criteria for:

(a) Remediation versus tolerance
(b) Public acknowledgment versus silence
(c) Legal escalation versus engagement

CATEGORY CC: FLOODGATE PROXY INFRASTRUCTURE

REQUEST NO. 24: Complete architectural and operational documentation of the Floodgate proxy infrastructure during the relevant period, including:

(a) Network topology (ingress points, backend routing, egress points)
(b) The list of client identifiers (device UDID, Apple ID, installation ID) attached to each proxied connection
(c) The retention policy for proxy logs
(d) Every backend system that reads proxy logs (for analytics, training, billing, or any other purpose)

Evidentiary predicate: Ex. F-4 at p. 22, l. 2 documents the proxy architecture.

REQUEST NO. 25: Complete per-session Floodgate proxy logs for every session originating from Plaintiff's Apple account during the relevant period,

produced with: (a) client identifier attached; (b) upstream provider contacted; (c) byte counts; (d) retention status.

REQUEST NO. 26: All documents regarding Apple's contractual and operational relationship with each upstream provider reached through the Floodgate proxy, including:

(a) Anthropic PBC
(b) OpenAI, Inc.
(c) Any additional provider
(d) The data-sharing, joint-controllership, or independent-processor characterization applicable to each

REQUEST NO. 27: All communications between Apple and each Floodgate-reached provider regarding Plaintiff, Plaintiff's Apple account, Plaintiff's devices, or Plaintiff's session data during the relevant period.

PHASE D: iCLOUD SYNC AND MESSAGES RETENTION (21 DAYS)

Counts developed by this Phase: Compl., Count XII (ECPA, 18 U.S.C. § 2511), Compl., Count XIV (CCPA / State Privacy), Compl., Count IX (Breach of Contract).

CATEGORY DA: UNAUTHORIZED iCLOUD SYNCHRONIZATION

REQUEST NO. 28: Complete documentation of the iCloud-synchronization behavior applied to AI-conversation, Xcode session, and Messages content during the relevant period, including:

(a) The complete list of content categories eligible for iCloud synchronization
(b) The consent and notice regime applicable to each category
(c) The default on/off state for each category at each OS version
(d) The per-content-category retention policy on iCloud servers

Evidentiary predicate: Ex. F-2 at p. 10, l. 2 documents unauthorized iCloud synchronization of AI-conversation content.

REQUEST NO. 29: Complete records of every iCloud synchronization event originating from Plaintiff's devices during the relevant period, with: (a) the content synchronized; (b) the iCloud container destination; (c) the per-event consent state; (d) the server-side retention.

REQUEST NO. 30: All documents regarding the decision to default iCloud synchronization to "on" for AI-conversation content (or to leave such content subject to the general default), including:

(a) The design-review records
(b) Any internal communications acknowledging that default-on synchronization would foreclose per-conversation user choice
(c) Any customer-facing disclosure of the behavior

CATEGORY DB: MESSAGES CONTAINER LITIGATION RETENTION

REQUEST NO. 31: Complete documentation of the Messages container retention regime during the relevant period, including:

(a) The architectural design of Messages container persistence on device
(b) The standard retention period for each category of Messages content
(c) The differential retention behavior documented at Ex. F-27 at p. 119, l. 2 (148 days retention of ostensibly-deleted content)
(d) Every trigger, flag, or rule that extends retention beyond the standard period

Evidentiary predicate: Ex. F-27 at p. 119, l. 2 documents 148-day litigation-document retention in the Messages container after user deletion.

REQUEST NO. 32: All documents regarding the design of the Messages container's deletion-semantics, including:

(a) The difference between "deleted" as presented to the user and the actual on-device state
(b) The server-side state following user-initiated deletion
(c) Any litigation or compliance-hold capability that prevents deletion
(d) Any legal review of the consumer-protection implications of the deletion-semantics gap

REQUEST NO. 33: Complete records of every Messages-container retention decision applied to Plaintiff's Messages during the relevant period, with: (a) the original message; (b) the user-initiated deletion event (if any); (c) the on-device persistence state following deletion; (d) the server-side state.

CATEGORY DC: MESSAGES CONTAINER VERIFICATION EXTRACTION

REQUEST NO. 34: Complete documentation of the extraction methodology verified at Ex. F-28 at p. 128, l. 2 and all internal Apple response, including:

(a) Any internal acknowledgment of the extraction's reproducibility
(b) Any remediation plan
(c) Any communication with law enforcement or regulatory bodies regarding the finding

REQUEST NO. 35: All documents regarding Apple's knowledge of third-party extraction tools capable of recovering Messages content past user-initiated deletion, and Apple's response to each such tool.

PHASE E: BIOME USER ACTIVITY TRACKING (21 DAYS)

Counts developed by this Phase: Compl., Count XII (ECPA, 18 U.S.C. § 2511), Compl., Count XIV (CCPA / State Privacy), Compl., Count X (Consumer Protection / Deceptive Trade Practices).

CATEGORY EA: BIOME DATABASE

REQUEST NO. 36: Complete documentation of the Biome / Core Knowledge database architecture deployed on macOS and iOS during the relevant period, including:

(a) The complete schema (entities, relationships, event types)
(b) The ingestion pipeline (OS hooks, application hooks, user-triggered vs. automatic)
(c) The retention policy per entity type
(d) The backend systems that read Biome contents (Siri, Proactive suggestions, Apple Intelligence, system-level analytics)

Evidentiary predicate: Ex. F-9 at p. 44, l. 2 documents Biome as user-activity tracking infrastructure.

REQUEST NO. 37: Complete Biome database snapshots for every device associated with Plaintiff's Apple account during the relevant period, produced in native format.

REQUEST NO. 38: All documents regarding customer-facing disclosure (or absence thereof) of Biome's existence, scope, and content-retention behavior, including:

(a) Privacy Policy language
(b) In-product settings exposing Biome-related controls
(c) Help Center or documentation-site pages

(d) App Store Privacy Nutrition Label filings referencing Biome-equivalent data

CATEGORY EB: SAFARI HISTORY CAPTURES CLAUDE URLS

REQUEST NO. 39: Complete documentation of the Safari-history → Biome ingestion pipeline during the relevant period, including:

(a) The source code for the ingestion

(b) The categorization logic applied to captured URLs

(c) Any differential treatment of AI-provider URLs (claude.ai, chat.openai.com, gemini.google.com)

Evidentiary predicate: Ex. F-19 at p. 84, l. 2 documents Safari-history capture of Claude URLs in Biome.

REQUEST NO. 40: Complete Safari-history-derived Biome records associated with Plaintiff's Apple account during the relevant period, produced in native format.

CATEGORY EC: BIOME CRASH LOGS TRACK CLAUDE DESKTOP

REQUEST NO. 41: Complete documentation of the Biome crash-log pipeline during the relevant period, including:

(a) The source code for crash-log ingestion into Biome

(b) The trigger conditions for crash-log recording

(c) Any differential treatment of third-party AI applications (Claude Desktop, ChatGPT, Perplexity)

(d) The downstream consumers of Biome crash-log content

Evidentiary predicate: Ex. F-20 at p. 88, l. 2 documents that Biome crash logs track Claude Desktop application activity.

REQUEST NO. 42: Complete Biome crash-log records associated with Plaintiff's devices and with the Claude Desktop application during the relevant period.

REQUEST NO. 43: All documents regarding the decision to capture crash-log telemetry for third-party applications into the Biome user-activity-tracking database, including:

(a) The rationale for coupling crash telemetry with activity tracking
(b) Any customer-facing disclosure of the coupling
(c) Any response to Plaintiff's forensic finding regarding the coupling

PHASE F: HIDDEN DECEPTION INSTRUCTIONS (14 DAYS)

Counts developed by this Phase: Compl., Count X (Consumer Protection / Deceptive Trade Practices), Compl., Count V (42 U.S.C. § 1985 Conspiracy).

CATEGORY FA: HIDDEN SYSTEM-PROMPT DECEPTION INSTRUCTIONS

REQUEST NO. 44: The complete text of every system-prompt, pre-prompt, or instruction injected by Xcode Intelligence, Apple Intelligence, or any Apple-operated AI integration into requests routed to any model provider during the relevant period, including:

(a) Every version of every instruction
(b) The commit and author for each instruction
(c) Any differential instruction applied based on user, account tier, or device configuration

Evidentiary predicate: Ex. F-1 at p. 5, l. 2 documents hidden deception instructions embedded in the system prompts Apple sends to AI providers.

REQUEST NO. 45: All documents regarding the design, authorization, and deployment of each deception instruction identified at Ex. F-1 at p. 5, l. 2, including:

(a) Who authored the instruction
(b) Who approved deployment

(c) The purpose of the instruction (whether to modify user experience, conceal model capabilities, conceal the model identity, or other)
(d) Any legal or policy review
(e) Any customer-facing disclosure

REQUEST NO. 46: All communications between Apple personnel and any model-provider counterparty regarding:

(a) The content of hidden system-prompt instructions
(b) The effect of such instructions on model output
(c) Any coordination regarding consistent deception instructions across providers
(d) Any discussion of the customer-protection or regulatory implications

CATEGORY FB: CLAUDE'S ADMISSION OF DECEPTION

REQUEST NO. 47: All documents regarding the API-request-and-response cycle documented at Ex. F-14 at p. 63, l. 2, in which Claude (the Anthropic model invoked via Apple's IDELanguageModelKit) admitted the presence of deception instructions in the system prompt, including:

(a) Apple's internal response to the admission
(b) Any remediation or instruction modification deployed in response
(c) Any communication with Anthropic regarding the admission
(d) Any customer-facing notification

REQUEST NO. 48: All internal documents acknowledging that Apple's hidden system-prompt instructions constitute misrepresentation or deception of the end user.

REQUEST NO. 49: All records of model-response events on Plaintiff's devices during the relevant period in which the invoked model emitted output suggesting awareness of, or resistance to, Apple-injected instructions.

PHASE G: SMOOTML ANALYTICS (14 DAYS)

Counts developed by this Phase: Compl., Count X (Consumer Protection / Deceptive Trade Practices), Compl., Count XII (ECPA, 18 U.S.C. § 2511), Compl., Count XIV (CCPA / State Privacy), Compl., Count XV (App Store Misrepresentation).

CATEGORY GA: SMOOTML UNDISCLOSED DATA COLLECTION

REQUEST NO. 50: Complete documentation of SmootML as deployed on macOS and iOS during the relevant period, including:

(a) The SmootML binary inventory and source code
(b) The complete event schema and per-event attribute payload
(c) The endpoint(s) to which SmootML transmits
(d) The retention policy at each destination
(e) The customer-facing disclosure (or absence thereof) of SmootML's existence and scope

Evidentiary predicate: Ex. F-12 at p. 55, l. 2 documents SmootML's undisclosed data-collection behavior.

REQUEST NO. 51: All SmootML event records attributable to Plaintiff's devices during the relevant period, produced as native JSON with full attribute payloads.

REQUEST NO. 52: All documents describing the relationship between SmootML and Apple's publicly-disclosed analytics practices, including:

(a) Whether SmootML is a subset of, superset of, or disjoint from the Apple analytics opt-in
(b) The effect of the Apple analytics opt-out on SmootML transmission
(c) Any customer-facing dialog controlling SmootML

CATEGORY GB: 189 CONNECTIONS PER SESSION

REQUEST NO. 53: Complete documentation of the SmootML-per-session connection architecture during the relevant period, including:

(a) The rationale for per-session connection establishment (rather than connection reuse)

(b) The keep-alive and connection-pooling configuration

(c) Any differential behavior based on user, account, or device identity

Evidentiary predicate: Ex. F-23 at p. 101, l. 2 documents 189 SmootML analytics connections per session.

REQUEST NO. 54: All documents regarding the decision to maintain the per-session connection count at its observed level, including any internal analysis of:

(a) The bandwidth and battery impact on users

(b) The analytics-granularity benefit justifying the bandwidth cost

(c) Any user-facing disclosure of per-session connection count

CATEGORY GC: DAILY ANALYTICS DURING AI USAGE

REQUEST NO. 55: Complete documentation of the daily-analytics collection differential observed during AI usage, including:

(a) The source code for the daily-analytics uplink

(b) Any differential in analytics volume when AI features are active versus inactive

(c) The backend systems that consume daily-analytics data

Evidentiary predicate: Ex. F-11 at p. 52, l. 2 documents the differential.

REQUEST NO. 56: Complete daily-analytics records for Plaintiff's devices during the relevant period, produced with per-day volume and endpoint distribution.

PHASE H: SOURCE CODE AND FILE PATH EXPOSURE (14 DAYS)

Counts developed by this Phase: Compl., Count XII (ECPA, 18 U.S.C. § 2511), Compl., Count IX (Breach of Contract).

CATEGORY HA: SOURCE CODE AND FILE PATH EXPOSURE

REQUEST NO. 57: Complete documentation of the file-path exposure architecture operative during the relevant period, including:

(a) The complete set of endpoints, logs, and telemetry channels that receive absolute file paths from user devices

(b) The scope of path exposure (user home directory name, project names, sensitive directory names)

(c) The retention policy at each destination

Evidentiary predicate: Ex. F-3 at p. 17, l. 2 documents source-code and file-path exposure via Xcode Intelligence and associated subsystems.

REQUEST NO. 58: All records of file-path exposure events originating from Plaintiff's devices during the relevant period.

REQUEST NO. 59: All documents regarding the privacy review of file-path exposure, including:

(a) Any analysis of re-identification risk from path components

(b) Any acknowledgment that user home directory names reveal identity

(c) Any customer-facing disclosure of the behavior

CATEGORY HB: SYSTEM PERMISSIONS AND ACCESS CONTROL

REQUEST NO. 60: Complete documentation of the macOS entitlements, TCC permissions, and sandbox profiles applied to each Apple Intelligence and Xcode Intelligence component during the relevant period, including:

(a) The full set of entitlements requested by each component
(b) The effective permission grants on user devices
(c) Any TCC database entries created without explicit user approval
(d) Any mechanism that bypasses or pre-approves TCC prompts

Evidentiary predicate: Ex. F-5 at p. 29, l. 2 documents the system-permissions and access-control architecture.

REQUEST NO. 61: Complete TCC database snapshots from Plaintiff's devices during the relevant period.

REQUEST NO. 62: All documents regarding Apple's use of private entitlements (unavailable to third-party developers) to grant Apple-operated AI components privileges beyond what user-facing consent dialogs disclose.

PHASE I: SYSTEM LOGGING AND TELEMETRY BLOCKING (14 DAYS)

Counts developed by this Phase: Compl., Count X (Consumer Protection / Deceptive Trade Practices), Compl., Count IX (Breach of Contract).

CATEGORY IA: MACOS SYSTEM SERVICE LOGGING

REQUEST NO. 63: Complete documentation of macOS system-service logging behavior during the relevant period with respect to AI activity, including:

(a) The system services that log AI-related events (`os_log`, unified logging, private data redaction)
(b) The log-retention policy per subsystem
(c) Any differential logging for AI events versus other system activity
(d) The backend systems that consume unified-logging data

Evidentiary predicate: Ex. F-7 at p. 37, l. 2 documents system-service logging of AI activity.

REQUEST NO. 64: Complete unified-logging records from Plaintiff's devices during the relevant period for the subsystems related to Apple Intelligence, Xcode Intelligence, IDELanguageModelKit, and ExternalModelService.

CATEGORY IB: USER TELEMETRY BLOCKING (HOSTS FILE)

REQUEST NO. 65: Complete documentation of Apple's response to users who attempt to block Apple telemetry through the system hosts file, including:

(a) Any mechanism that overrides hosts-file entries
(b) Any mechanism that detects hosts-file modification
(c) Any analytics that flag devices with modified hosts files
(d) Any differential treatment (in feature availability, account standing, or otherwise) of devices with modified hosts files

Evidentiary predicate: Ex. F-25 at p. 109, l. 2 documents Apple's detection and circumvention of user telemetry-blocking attempts.

REQUEST NO. 66: All documents regarding the design decision to detect and circumvent user hosts-file modifications, including the stated rationale and any legal review.

CATEGORY IC: APPLE INTELLIGENCE PRIVACY DISCLOSURES

REQUEST NO. 67: Complete documentation of Apple's privacy-disclosure regime for Apple Intelligence during the relevant period, including:

(a) The marketing materials (web, in-product, press-release) representing Apple Intelligence's privacy properties
(b) The keynote and WWDC session language representing on-device versus cloud processing
(c) The Private Cloud Compute architectural claims and any deviations in the actual deployed architecture
(d) Any internal acknowledgment of a gap between disclosed and actual privacy behavior

Evidentiary predicate: Ex. F-26 at p. 113, l. 2 documents the disclosure regime and its deviations from observed behavior.

REQUEST NO. 68: All internal documents analyzing whether Apple's Apple Intelligence privacy representations comply with:

(a) App Store Review Guideline 5 (Legal) and associated Privacy Nutrition Label requirements
(b) Federal Trade Commission Act Section 5 (unfair or deceptive practices)
(c) California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)
(d) State data-privacy laws generally

PHASE J: SOURCE-CODE CROSS-VERIFICATION AND CROSS-DEFENDANT COORDINATION (21 DAYS)

Counts developed by this Phase: Compl., Count V (42 U.S.C. § 1985 Conspiracy), Compl., Count VI (RICO, 18 U.S.C. § 1962), Compl., Count XII (ECPA, 18 U.S.C. § 2511).

CATEGORY JA: SOURCE-CODE CROSS-VERIFICATION

REQUEST NO. 69: All documents regarding Apple's internal response to the source-code-cross-verification findings set out at Ex. F-29 at p. 133, l. 3, including:

(a) Any acknowledgment of the findings
(b) Any remediation plan

(c) Any communication with counsel regarding disclosure obligations triggered by the findings

REQUEST NO. 70: Complete source code for the components cross-verified at Ex. F-29 at p. 133, l. 3, including Xcode Intelligence, Apple Intelligence, IDELanguageModelKit, and ExternalModelService, in every version deployed during the relevant period.

CATEGORY JB: APPLE-OPENAI PARTNERSHIP

REQUEST NO. 71: Complete documentation of the Apple-OpenAI partnership integration during the relevant period, including:

(a) The complete partnership contract and any amendments
(b) The data-processing and joint-controllership characterization
(c) The set of user-data categories flowing from Apple to OpenAI and vice versa
(d) The billing, revenue-share, or consideration flow between the parties

Evidentiary predicate: Cross-reference Ex. G-4 at p. 24, l. 2.

REQUEST NO. 72: All communications between Apple and OpenAI regarding Plaintiff, Plaintiff's Apple account, Plaintiff's devices, or Plaintiff's session data during the relevant period.

CATEGORY JC: APPLE-ANTHROPIC COORDINATION

REQUEST NO. 73: Complete documentation of any integration, partnership, or data-sharing arrangement between Apple and Anthropic PBC during the relevant period, whether characterized as a formal partnership, an API integration, a research collaboration, or otherwise, including:

(a) Every contract, memorandum of understanding, and term sheet
(b) The data-processing characterization applicable to each flow

(c) The set of user-data categories flowing in each direction

(d) Any joint-analytics or cross-analytics arrangement

REQUEST NO. 74: All communications between Apple and Anthropic PBC regarding Plaintiff, Plaintiff's Apple account, or Plaintiff's devices during the relevant period.

REQUEST NO. 75: All documents regarding the Apple-Anthropic integration architecture documented in the March 31, 2026 Anthropic source-code release (Ex. E-32 at p. 235, l. 3), including:

(a) Apple's knowledge of the integration as disclosed in the Leaked Source

(b) Apple's internal response to the Leak

(c) Any coordination with Anthropic regarding post-leak rotation of shared credentials or endpoints

CATEGORY JD: XPROTECT / DATAEXFIL.KEYCHAIN

REQUEST NO. 76: Complete documentation of XProtect detections classified as `DataExfil.Keychain` or any related DataExfil signature during the relevant period, including:

(a) The signature definitions

(b) The detection events generated per device

(c) Any detection event generated on Plaintiff's devices

(d) The response protocol (remediation, user notification, backend escalation) associated with each signature

Evidentiary predicate: Cross-reference Ex. E-16 at p. 120, l. 2 documents Apple's XProtect flagging of Claude for DataExfil.Keychain.

REQUEST NO. 77: All communications between Apple XProtect personnel and Anthropic PBC regarding the DataExfil.Keychain signature, its applicability to Anthropic products, and any remediation or tolerance decision.

CATEGORY JE: DATADOG SUBPROCESSOR — APPLE TELEMETRY PIPELINE

REQUEST NO. JE-1: Complete documentation of Apple's relationship with Datadog, Inc. (Delaware corporation; NASDAQ: DDOG) and its 100% Israeli subsidiary Datadog Israel Ltd. (Israeli Company Identification Number 516464922) during the relevant period, including: (a) the Data Processing Addendum, Master Subscription Agreement, Supplemental Terms, and any other contractual instruments; (b) the complete list of Apple services, applications, frameworks, and platform components that transmit telemetry, error reports, performance data, or other data to Datadog ingest endpoints — including without limitation any transmissions documented at the F-series Apple-code-forensics exhibits referenced at Memo C ¶¶ 64, 67 (ECF No. 51-3); (c) all hardcoded Datadog endpoints (IP addresses, hostnames, client tokens) embedded in Apple client binaries, libraries, frameworks, or backend infrastructure; (d) the configuration of the Datadog telemetry pipeline as deployed against Plaintiff's accounts, devices, and identifiers, including any per-user routing, sampling, or force-rule mechanisms; (e) all ingest records corresponding to events transmitted from Plaintiff's devices, identifiers, accounts, or sessions to any Datadog endpoint; and (f) all records governing affiliate-tier subprocessor

inheritance to Datadog Israel Ltd. with respect to Apple customer data and Apple platform telemetry.

Evidentiary predicate: Datadog, Inc. and Datadog Israel Ltd. are the same telemetry-subprocessor and patent-substrate dyad documented at Appendix P (ECF No. 51-26). Memo C ¶¶ 64, 67 (ECF No. 51-3) plead that the F-series Apple-code-forensics exhibits "establish parallel transmissions from Apple platform infrastructure" to Datadog. Discovery establishes whether Apple's data flows are subject to the same affiliate-inheritance access pattern alleged at App. P §§ I, II.B, V.D supporting Compl., Count V, Compl., Count VI, Compl., Count XII, and Compl., Count XIV.

REQUEST NO. JE-2: All communications (Slack, email, ticketing, project-management, code-review, design-document, contract-negotiation, and equivalent records) during the relevant period between Apple personnel and Datadog, Inc. (or Datadog Israel Ltd.) personnel concerning: (a) the design, deployment, modification, or operational integration of any Apple-Datadog telemetry pipeline; (b) any per-user routing, sampling, or differential treatment configurable through Datadog; (c) the affiliate-tier subprocessor inheritance structure; (d) Plaintiff or Plaintiff's account; (e) any of the OzCode-origin patents (U.S. Patent Nos. 10,783,055; 10,783,056; 10,789,151; 10,795,801; 10,990,504; 11,048,615; 11,080,164; and continuation US 2026/0072809 A1) and their applicability to Apple's runtime infrastructure; and (f) any joint-

data-processing arrangement between Apple and Datadog regarding Apple Intelligence partner data, Floodgate-routed traffic, or App Store telemetry.

PHASE K: CORPORATE / CONTRACTUAL / DEVELOPER PROGRAM (30 DAYS)

Counts developed by this Phase: Compl., Count IX (Breach of Contract), Compl., Count X (Consumer Protection / Deceptive Trade Practices).

CATEGORY KA: CORPORATE STRUCTURE AND AUTHORIZATION

REQUEST NO. 78: All documents sufficient to identify the Apple corporate structure, reporting lines, and senior authorization for each mechanism identified in Phases A through J, including:

(a) Executive-level approvals
(b) Product-leadership review
(c) Legal-review sign-offs
(d) Privacy-team review (the Office of the Chief Privacy Officer, if applicable)

CATEGORY KB: DEVELOPER PROGRAM AND ENTERPRISE

REQUEST NO. 79: Complete documentation of any Apple Developer Program, Enterprise Program, Education Program, or partnership arrangement applicable to Plaintiff's Apple account during the relevant period, including the terms governing:

(a) Apple's use of code or content transiting Apple services
(b) Apple's disclosure obligations
(c) Apple's audit and verification rights

REQUEST NO. 80: All communications between Apple and Plaintiff during the relevant period regarding Plaintiff's Developer Program status, Enterprise access, or any related arrangement.

PHASE L: CONSUMER-FACING AND PRIVACY NUTRITION LABEL (30 DAYS)

Counts developed by this Phase: Compl., Count X (Consumer Protection / Deceptive Trade Practices), Compl., Count XV (App Store Misrepresentation).

CATEGORY LA: PRIVACY NUTRITION LABEL FILINGS

REQUEST NO. 81: All Privacy Nutrition Label filings submitted by Apple Inc. for every Apple-developed application (including Xcode, macOS Writing Tools, Safari, Messages) during the relevant period, with per-version effective dates and internal approval records.

REQUEST NO. 82: All internal analysis regarding whether Apple's Privacy Nutrition Label filings accurately represent the data collection documented in Phases A through J, including any analysis acknowledging a gap.

CATEGORY LB: IN-PRODUCT AND MARKETING DISCLOSURES

REQUEST NO. 83: All in-product consent modals, settings dialogs, onboarding flows, and help-center articles operative during the relevant period that address AI-feature data collection, including per-version text and effective dates.

REQUEST NO. 84: All marketing materials (web pages, emails, video advertisements, keynote transcripts, press releases) that reference privacy properties of Apple Intelligence, Xcode Intelligence, or any AI integration during the relevant period.

PHASE M: PRESERVATION AND EXPERT DISCLOSURE (IMMEDIATE / 30 DAYS)

CATEGORY MA: PRESERVATION

REQUEST NO. 85: Complete documentation of every preservation hold, litigation hold, or legal hold issued by Apple during the relevant period, including scope, custodians, effective dates, and compliance audits.

REQUEST NO. 86: All documents regarding destruction, deletion, overwriting, or spoliation of electronically stored information during the pendency of any preservation hold identified in REQUEST NO. 85.

REQUEST NO. 87: Complete documentation of Apple's ESI retention infrastructure during the relevant period, including automated retention policies, backup/replication infrastructure, and deletion schedules for each category of data identified in Phases A through L.

CATEGORY MB: EXPERT AND FACT WITNESSES

REQUEST NO. 88: Identify every person employed by or contracting with Apple who has personal knowledge of the authorship, authorization, deployment, or operation of any mechanism identified in Phases A through L, together with each person's role, employment period, and current employment status.

REQUEST NO. 89: Identify every expert witness Apple intends to offer on any subject addressed in Phases A through L, together with qualifications, prior testimony, and preliminary opinions.

REQUEST NO. 90: All communications with any third-party consultant, outside auditor, or expert retained by Apple to analyze, audit, or opine on any

mechanism identified in Phases A through L, whether or not disclosed as a testifying expert.

PRESERVATION NOTICE

This request serves as express notice under Federal Rule of Civil Procedure 37(e) that Defendant Apple Inc. is on notice of the following categories of electronically stored information (ESI) subject to preservation obligation pending completion of production. Routine destruction of any of these categories is expressly prohibited:

1. All versions of `IDELanguageModelKit.framework` and `ExternalModelService` binaries and source code deployed during the relevant period.

2. All Floodgate proxy logs attributable to Plaintiff's Apple account.

3. All iCloud container contents, Messages container snapshots, and Biome database snapshots associated with Plaintiff's Apple account.

4. All OAuth tokens and Xcode cache artifacts on or derived from Plaintiff's devices.

5. All hidden system-prompt instruction texts, in every version deployed during the relevant period.

6. All communications with Anthropic PBC, OpenAI, Inc., and any other AI-model-provider counterparty regarding Plaintiff, Plaintiff's account, or Plaintiff's devices.

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