

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

JOSEPH KIRCHNER,

Plaintiff,

v.

MIKE JOHNSON, in his individual and official
capacity as Speaker of the United States House of
Representatives;
DONALD J. TRUMP, in his individual capacity as
former and current President of the United States;
PAM BONDI, in her individual and official
capacity as Attorney General of the United States;
BRENDAN CARR, in his individual and official
capacity as Chairman of the Federal
Communications Commission;
THE UNITED STATES HOUSE OF
REPRESENTATIVES;
ANTHROPIC PBC;
OPENAI, INC.;
APPLE INC.;
COMCAST CABLE COMMUNICATIONS, LLC;
METR (MODEL EVALUATION & THREAT
RESEARCH);
and DOES 1-20, unknown co-conspirators,
Defendants.

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

**EXHIBIT G: OPENAI
CODE FORENSICS**

TABLE OF CONTENTS

OpenAI Evidence Executive Summary	1
G-1: ChatGPT Atlas Comprehensive Forensic Analysis.....	1
G-2: ChatGPT iOS Forensic Analysis	14
G-3: ChatGPT Desktop Network Forensics	18
G-4: Apple OpenAI Partnership Integration.....	23
G-5: OpenAI Privacy Nutrition Label Analysis	27

OpenAI Evidence Executive Summary

OVERVIEW

Exhibit Series G documents forensic analysis of OpenAI's ChatGPT products — ChatGPT Atlas (macOS desktop) and ChatGPT iOS — conducted in December 2025. The evidence establishes a comparative baseline for industry telemetry practices, documenting multi-layered tracking infrastructure, asymmetric certificate pinning between platforms, and OS-level integration with Apple Intelligence.

Source documentation for each exhibit is filed separately on USB. The evidence/subdirectory path for each exhibit is noted in its corresponding footnote.

CITED BY PLEADINGS

This exhibit (G-0) is cited by the following pleadings in the filing record:

Pleading	Cites	Paragraphs
Third Amended Complaint	1	¶ 58

Total: 1 citation(s) across 1 pleading(s).

G-1: ChatGPT Atlas Comprehensive Forensic Analysis

For legal analysis applying the ChatGPT Atlas forensic findings — 470 MB across 6 storage locations, 4 persistent device identifiers, 61+ Segment events, 4 third-party analytics providers — as the industry comparative baseline to the causes of action, see:

- *Memo A ¶ 40 — § IV.D OpenAI Comparative Baseline*
- *See — § IV.D Atlas as disclosed-but-aggressive baseline (Counts X and XIV)*

A - EXECUTIVE SUMMARY

Forensic analysis of ChatGPT Atlas reveals a sophisticated multi-layered telemetry infrastructure that:

1. Stores approximately 470 MB of user data across 6+ distinct storage locations
2. Maintains 4 separate persistent device identifiers for cross-session tracking
3. Records 61+ Segment analytics events with persistent anonymous IDs
4. Stores user email in plaintext in unencrypted preference files
5. Tracks 40+ specific user behaviors with Unix timestamps
6. Transmits data to 4 third-party analytics providers: Statsig, Sentry, Segment, and Datadog
7. Implements "Work with Apps" file access through 30+ connector integrations

B - APPLICATION TECHNICAL PROFILE**Application Identification:**

Attribute	Value	Source
Application Name	ChatGPT Atlas	Application bundle
Bundle Identifier	com.openai.atlas	Info.plist
Version	1.2025.344.7	Preferences plist
Build Number	20251218120745000	SEGBuildKeyV2
Release Date	December 18, 2025	Build timestamp
Environment	production-macos	Sentry session

Technical Architecture:

Component	Implementation
Native Layer	Swift application
Web Runtime	Chromium 143.0.7499.110
Bridge Framework	OwlBridge.framework
Crash Reporter	Sentry.framework (bundled)
Image Cache	Kingfisher framework
Update System	Sparkle (SUAutomaticallyUpdate)

¹ Source documentation filed separately on USB. Path: DDC_EVIDENCE/4_Code Forensics/EXHIBIT_G_OPENAI/G_chatgpt_atlas_comprehensive_forensic/evidence/

Application Bundle Location:**File: bundle_structure.txt**

```

1 | /Applications/ChatGPT Atlas.app/
2 | └─ Contents/
3 |     └─ Frameworks/
4 |         └─ Sentry.framework           ← Bundled telemetry
5 |         └─ OwlBridge.framework       ← Chromium bridge
6 |         └─ [additional frameworks]
7 |     └─ Support/
8 |         └─ ChatGPT Atlas.app/        ← Nested Chromium app
9 |     └─ Info.plist

```

C - DATA STORAGE INVENTORY**Complete Storage Location Map:**

#	Location	Size	Purpose
1	~/Library/Application Support/com.openai.atlas/	136 MB	Primary data
2	~/Library/Application Support/OpenAI/	~0	Native messaging
3	~/Library/Caches/com.openai.atlas/	333 MB	Browser cache
4	~/Library/HTTPStorages/com.openai.atlas/	488 KB	HTTP data
5	~/Library/Preferences/com.openai.*.plist	~7 KB	Preferences
6	~/Library/Preferences/com.segment.storage.oai.plist	~1 KB	Segment data
TOTAL		~470 MB	

Primary Data Directory Structure:

File: directory_structure.txt

```

1|com.openai.atlas/ [136 MB total]
2|├─ browser-data/ [~80 MB]
3|   └─ host/
4|       ├─ debug.log [90 KB - network logs]
5|       ├─ Local State [28 KB - config JSON]
6|       └─ user-CKysnbNDz3G9BBTWYHbThPk1__a183ed1b-39bd-4a8c-99f0-
7|           └─ IndexedDB/
8|               └─ https_chatgpt.com_0.indexeddb.leveldb/
9|               └─ Local Storage/
10|                  └─ leveldb/
11|├─ conversations-v3-a183ed1b-39bd-4a8c-99f0-1e1172ecb41f/ [14 MB]
12|   └─ 682c8920-5a2c-8011-ac8a-24fa27fba915.data [1.4 MB - encrypted]
13|       └─ [20 additional .data files]
14|├─ io.sentry/ [Session telemetry]
15|   └─ INSTALLATION [Device ID]
16|       └─ SentryCrash/
17|├─ statsig/ [2.7 MB]
18|   └─ com.statsig.cache.data [Feature flags cache]
19|└─ suggestions-cache/ [Hash-named files]

```

D - TELEMETRY PROVIDER ANALYSIS**Provider Overview:**

Provider	Evidence Location	Data Type
Statsig	statsig/, preferences	Feature flags, A/B testing
Sentry	io.sentry/, framework	Crash reports, sessions
Segment	com.segment.storage.oai.plist	Behavioral analytics
Datadog	debug.log references	Real User Monitoring

Statsig Implementation:

- Cache File: ~/Library/Application Support/com.openai.atlas/statsig/com.statsig.cache.data
- Size: 2.7 MB
- Format: Encrypted/compressed binary
- Preferences Key: com.Statsig.InternalStore.stableIDKey
- Value: 57938EBA-8EBF-40CB-9425-3ECE3A3C9D41

Sentry Implementation:

- Framework Location: /Applications/ChatGPT
Atlas.app/Contents/Frameworks/Sentry.framework

• Data Directory: ~/Library/Application Support/com.openai.atlas/io.sentry/
Sentry Installation ID File:

File: INSTALLATION

1|393445FD-153B-47C0-8814-F958F06C0093

Datadog Evidence from debug.log:

File: debug.log

1|[61418:4688296:1222/120734.727216:INFO:CONSOLE:7] "Datadog Browser SDK:
 2|Customer data exceeds the recommended 3KiB threshold. More details:
 3|https://docs.datadoghq.com/real_user_monitoring/browser/troubleshooting/
 4|#customer-data-exceeds-the-recommended-threshold-warning",
 5|source: https://auth-cdn.oaistatic.com/assets/datadog-BTgRrIvw.js (7)

E - DEVICE FINGERPRINTING EVIDENCE

Complete Device Identifier Inventory:

#	Identifier Name	Value	Location	Purpose
1	Sentry Device ID	393445FD-153B-47C0-8814-F958F06C0093	io.sentry/INSTALLATION	Crash correlation
2	Statsig Stable ID	57938EBA-8EBF-40CB-9425-3ECE3A3C9D41	com.openai.atlas.plist	A/B testing
3	Device ID Backup	CF84FE22-2B93-4AF5-977B-4488BA4F42A4	com.openai.atlas.plist	Redundant tracking
4	Segment Anonymous ID	394F3C24-E247-4BE8-9E4C-DA85B977947C	com.segment.storage.oai.plist	Analytics
5	Machine ID	7372387	Local State JSON	Hardware ID
6	Entropy Source	FA9CDB724C88B7F47EB1128E79EDD738	Local State JSON	Randomization

Machine ID and Entropy Source Evidence:

File: Local_State.json

```

1 {
2   "machine_id": 7372387,
3   "pseudo_low_entropy_source": 4260,
4   "low_entropy_source3": 2810,
5   "limited_entropy_randomization_source": "FA9CDB724C88B7F47EB1128E79EDD738"
6 }

```

F - SEGMENT ANALYTICS DEEP DIVE
Segment Storage File Analysis:**File: com.segment.storage.oai.plist**

```

1 {
2   "segment.anonymousId" => "394F3C24-E247-4BE8-9E4C-DA85B977947C"
3   "segment.events" => 61
4   "segment.settings" => {length = 124, bytes = 0x626c7330d126974...
5   "segment.traits" => {length = 504, bytes = 0x626c7330dc246... 000000198}
6   "segment.userId" => "user-CKysnbNDz3G9BBTWYHbThPkl"
7 }

```

Segment Data Fields Explained:

Field	Value	Meaning
segment.anonymousId	UUID	Persistent ID before login
segment.events	61	Total events tracked
segment.settings	124 bytes binary	Configuration data
segment.traits	504 bytes binary	User characteristics
segment.userId	user-CKysnbNDz3G9BBTWYHbThPkl	Authenticated user ID

G - STATSIG FEATURE FLAG SYSTEM
Statsig Service Configuration:

File: com.openai.chat.StatsigService.plist

```

1 {
2   "accountID" => "a183ed1b-39bd-4a8c-99f0-1e1172ecb41f"
3   "planType" => "team"
4   "userEmail" => "jdkirchner47@gmail.com"
5   "userID" => "user-CKysnbNDz3G9BBTWYHbThPk1"
6 }

```

CRITICAL FINDING: User email address stored in **plaintext** in unencrypted preference file.

Remote Feature Flags:**File: com.openai.chat.RemoteFeatureFlags.plist**

```

1 {
2   "appPairing" => true
3   "auraAvailable" => true
4   "disableModelUpsell" => true
5   "disableUpgradeUI" => true
6   "memoryAvailable" => true
7   "moonshine" => false
8   "searchTool" => true
9   "voiceAvailable" => true
10  "whisperKillswitch" => false
11 }

```

Feature Flag Definitions:

Flag	Value	Likely Purpose
appPairing	true	"Work with Apps" integration
auraAvailable	true	Unknown feature
memoryAvailable	true	Conversation memory
moonshine	false	Unknown (disabled)
searchTool	true	Web search capability
voiceAvailable	true	Voice input/output
whisperKillswitch	false	Speech-to-text active

H - SENTRY TELEMETRY INFRASTRUCTURE**Sentry Session Data:**

File: session.current

```

1{
2  "seq": 1,
3  "sid": "EBC5BD58-4F11-4E0E-8337-1BB58EF9946E",
4  "did": "393445FD-153B-47C0-8814-F958F06C0093",
5  "timestamp": "2025-12-22T19:03:50.146Z",
6  "status": "ok",
7  "started": "2025-12-22T19:03:50.145Z",
8  "attrs": {
9    "release": "com.openai.atlas@1.2025.344.7+20251218120745000",
10   "environment": "production-macos"
11 },
12 "errors": 0,
13 "init": true
14}

```

Sentry Session Fields Explained:

Field	Value	Meaning
seq	1	Sequence number
sid	EBC5BD58-4F11-4E0E-8337-1BB58EF9946E	Session ID
did	393445FD-153B-47C0-8814-F958F06C0093	Device ID
timestamp	2025-12-22T19:03:50.146Z	Session timestamp
release	com.openai.atlas@1.2025.344.7+20251218120745000	App version
environment	production-macos	Environment tag

Sentry Crash State:**File: CrashState.json**

```

1{
2  "version": 1,
3  "crashedLastLaunch": false,
4  "durationFromCrashStateInitToLastCrash": 0,
5  "activeDurationSinceLastCrash": 0,
6  "backgroundDurationSinceLastCrash": 0,
7  "launchesSinceLastCrash": 1,
8  "sessionsSinceLastCrash": 1
9}

```

I - NETWORK ENDPOINT ANALYSIS**OpenAI Domains:**

URL	Purpose
https://auth.openai.com/	Authentication
https://auth.openai.com/log-in	Login page
https://auth.openai.com/mfa-challenge/*	MFA verification
https://sentinel.openai.com/cdn-cgi/challenge-platform/scripts/jsd/main.js	Security sentinel
https://chatgpt.com/	Main application
https://chatgpt.com/ces/v1/projects/oai/settings	Analytics settings

Analytics Domains:

URL	Provider	Purpose
https://auth-cdn.oaistatic.com/assets/datadog-BTgRrIvw.js	Datadog	RUM analytics
https://auth-cdn.oaistatic.com/assets/segment-DbvycV5h.js	Segment	Behavioral tracking
https://auth-cdn.oaistatic.com/assets/app-core-BTg4Btsf.js	OpenAI	Core analytics

HTTP Storage Database Analysis:

Host	Alternate Host	Port	Creation Time	Expires Time
auth.openai.com	auth.openai.com	443	1766426945	1766513345
lh3.googleusercontent.com	lh3.googleusercontent.com	443	1766426953	1767031753
sdmntprnorthcentralus.oaiusercontent.com	sdmntprnorthcentralus.oaiusercontent.com	443	1766426995	1766513395
ws.chatgpt.com	ws.chatgpt.com	443	1766430703	1766517103
ios.chat.openai.com	ios.chat.openai.com	443	1766431228	1766517628

J - USER BEHAVIOR TRACKING**Behavior Timestamp Evidence (40+ tracked behaviors):**

Behavior Key	Timestamp	Human Readable
oai/apps/hasSeenOnboarding	748995615	Initial onboarding
oai/apps/hasSeenTeamOwnerOnboarding	748995605	Team setup
oai/apps/hasSeenTemporaryChatOnboarding	748998229	Temp chat intro
oai/apps/hasSeenMentionGPTs	749588863	GPT mentions
oai/apps/hasSeenMemoryOnboarding	749505305	Memory feature
oai/apps/hasSeenAdvancedVoice/2024-09-24	753681907	Voice features
oai/apps/hasSeenAppPairingOnboarding	753666904	Work with Apps
oai/apps/hasSeenProjectsWebNuxTooltip	756930049	Projects feature
oai/apps/hasSeenCanvasDropdownNux	749771296	Canvas feature
oai/apps/hasSeenCanvasCodeExecutionNux	762134435	Code execution
oai/apps/hasSeenO3MiniNux	760904307	o3-mini model
oai/apps/hasSeenConnectorsNuxModal	770831171	Connectors intro

User Settings Tracked:

File: user_settings.json

```
1|{
2|  "voiceName": "maple",
3|  "trainingAllowed": true,
4|  "moonshine": true,
5|  "chatTheme": "default",
6|  "voiceBackgroundEnabled": false,
7|  "kaur1br5ShareUsageLogsAllowed": true,
8|  "atlasAdultSearchAllowed": true,
9|  "lastUsedModelConfig": {
10|    "slugs": {
11|      "default": "gpt-5-2-pro",
12|      "web": "gpt-5-2-pro"
13|    }
14|  }
15|}
```

Settings Explained:

Setting	Value	Meaning
trainingAllowed	true	Data may be used for training
kaur1br5ShareUsageLogsAllowed	true	Usage logs shared
atlasAdultSearchAllowed	true	Adult content in search
lastUsedModelConfig.slugs.default	gpt-5-2-pro	Default model

K - FILE ACCESS INFRASTRUCTURE

"Work with Apps" Connector System (30+ total):

Connector ID	Description
connector:google_drive	Search within your apps
connector:onedrive	Search within your apps
connector:confluence	Search within your apps
connector:sharepoint	Search within your apps
connector:box	Search within your apps
connector:dropbox	Search within your apps
connector:notion	Search within your apps
connector:slack	Search within your apps
connector:github	Search within your apps
connector:jira	Search within your apps
connector:asana	Search within your apps
connector:linear	Search within your apps
connector:zendesk	Search within your apps
connector:intercom	Search within your apps
connector:salesforce	Search within your apps
connector:hubspot	Search within your apps

L - LOCAL STORAGE ENCRYPTION ANALYSIS

Conversation Data Encryption:

Directory: ~/Library/Application Support/com.openai.atlas/conversations-v3-/

Sample File: 682c8920-5a2c-8011-ac8a-24fa27fba915.data

Hexdump (first 64 bytes):

File: hexdump.txt

```

1|00000000: 5162 3a59 66df b516 7e14 9b86 e46c 2766 Qb:Yf...~....l'f
2|00000010: 4be6 1401 1603 08f9 3fb3 1ece dc30 22a3 K.....?....0".
3|00000020: [encrypted binary data continues]

```

Analysis: Data is **encrypted**, not base64 encoded. Cannot be decoded without encryption key.

IndexedDB LevelDB Content (partial - WebRTC certificates):**File: 000005.ldb**

```

1|BEGIN PRIVATE KEY
2|MIGHAgEAMBMGBYqGSM49AgEGCC...
3|END PRIVATE KEY
4|
5|BEGIN CERTIFICATE
6|MIIBFzCBvaADAgECAGkAub1KNGBfR5owCgYIKoZIzj0EAwIwETEPMA0GA1UEAwWG
7|V2ViUlRDMB4XDTI1MTIyMTE4MTAxMVoXDTI2MDEy...
8|END CERTIFICATE

```

M - CONCLUSIONS AND FINDINGS**Data Collection Summary:**

Category	Finding
Total Local Storage	~470 MB across 6+ locations
Device Identifiers	4 separate persistent IDs
Analytics Events	61+ Segment events tracked
Behavior Timestamps	40+ user actions timestamped
Third-Party Providers	4 (Statsig, Sentry, Segment, Datadog)
User PII Exposed	Email in plaintext preference file

Privacy Concerns Identified:

1. Plaintext Email Storage: User email stored in unencrypted
com.openai.chat.StatsigService.plist

2. Multiple Persistent Identifiers: Four separate device IDs enable cross-session and potentially cross-platform tracking

3. Extensive Behavior Tracking: 40+ specific user interactions timestamped and stored

4. Third-Party Data Sharing: Data transmitted to Statsig, Sentry, Segment, and Datadog

5. Datadog Data Volume: Warning indicates >3KB "customer data" per session

6. File Path Exposure: Local file paths stored in IndexedDB/Local Storage

Comparison with Claude Desktop:

Aspect	Claude Desktop	ChatGPT Atlas
Hidden Home Directory	Yes (~/.claude/)	No
Preference Files	Minimal	6 separate files
Local Encryption	No (Base64)	Yes (Binary)
Device IDs	1-2	4
User Email in Plaintext	Unknown	Yes
Behavior Timestamps	Unknown	40+
Total Storage	~50 MB	~470 MB
Third-Party Providers	3	4

CITED BY PLEADINGS

This exhibit (G-1) is cited by the following pleadings in the filing record:

Pleading	Cites	Paragraphs
Third Amended Complaint	2	¶ 33, ¶ 88
Memo A	2	¶ 40, ¶ 41
discovery_openai	3	¶ 1, ¶ 3

Total: 7 citation(s) across 3 pleading(s).

G-2: ChatGPT iOS Forensic Analysis

For legal analysis applying the ChatGPT iOS comparative forensics — no Sift Science, no Facebook SDK, fewer permissions, certificate pinning present — to the causes of action, see Memo A ¶ 40 (§ IV.D OpenAI Comparative Baseline — defeats "industry standard" defense).

A - CERTIFICATE PINNING IMPLEMENTATION

ChatGPT iOS implements certificate pinning on authentication endpoints:

PINNED ENDPOINTS:

Endpoint	Status
ios.chat.openai.com	PINNED
ab.chatgpt.com	PINNED
api.openai.com	Partial

EVIDENCE (mitmproxy log):

File: mitmproxy.log

```
1|[04:48:14.861] Client TLS handshake failed. The client disconnected
2|during the handshake. If this happens consistently for
3|ios.chat.openai.com, this may indicate that the client does not
4|trust the proxy's certificate.
```

SECURITY IMPLICATION:

Certificate pinning prevents man-in-the-middle attacks, protecting user credentials and conversation data in transit.

Claude iOS does NOT implement certificate pinning.

B - NO SIFT SCIENCE INTEGRATION

ChatGPT iOS does NOT integrate Sift Science fraud detection:

² Source documentation filed separately on USB. Path: DDC_EVIDENCE/4_Code Forensics/EXHIBIT_G_OPENAI/G_chatgpt_ios_forensic_analysis/evidence/

SDK COMPARISON:

Third-Party SDK	ChatGPT iOS	Claude iOS
Sift Science	NO	YES
Facebook/Meta SDK	NO	YES
Firebase	NO	YES
Google Sign-In	NO	YES

SIGNIFICANCE:

AI assistants can function without surveillance-grade fraud detection. Claude's Sift Science integration collects 38+ network IP addresses, device info, and behavioral data - ChatGPT achieves equivalent functionality without this surveillance.

C - PERMISSION SCOPE COMPARISON

ChatGPT iOS requests FEWER permissions than Claude iOS:

Permission	ChatGPT iOS	Claude iOS
Camera	YES	YES
Microphone	YES	YES
Location (When In Use)	YES	YES
Photos	YES	YES
Calendar (Full Access)	NO	YES
Reminders (Full Access)	NO	YES

Summary:

- ChatGPT requests: 4 permissions
- Claude requests: 6 permissions

SIGNIFICANCE:

AI assistants can provide equivalent functionality without full access to personal scheduling data.

D - PRIVACY MANIFEST COMPLIANCE

ChatGPT iOS contains 18 privacy manifest files with full disclosure:

ALL DETECTED SDKs DISCLOSED:

SDK	Detected	Disclosed	Purpose
Segment	YES	YES	Analytics
Sentry	YES	YES	Crash reporting
Datadog	YES	YES	Monitoring
Stripe	YES	YES	Payments
RevenueCat	YES	YES	Subscriptions
Auth0	YES	YES	Authentication
LiveKit	YES	YES	Voice/Video

NSPrivacyTracking: false (all manifests)

UNDISCLOSED THIRD PARTIES: 0

E - COMPREHENSIVE COMPARISON

ChatGPT iOS vs Claude iOS - Privacy and Security:

Category	ChatGPT iOS	Claude iOS	Winner
Third-party SDKs	7	9+	ChatGPT
Undisclosed data sharing	0	2+	ChatGPT
Permissions requested	4	6	ChatGPT
Certificate pinning	YES	NO	ChatGPT
Privacy manifest compliance	Full	Partial	ChatGPT
Fraud detection surveillance	NO	YES	ChatGPT

ChatGPT iOS wins ALL privacy/security categories.

CITED BY PLEADINGS

This exhibit (G-2) is cited by the following pleadings in the filing record:

Pleading	Cites	Paragraphs
Third Amended Complaint	2	¶ 33, ¶ 88
Memo A	1	¶ 40
discovery_openai	5	¶ 1, ¶ 3

Total: 8 citation(s) across 3 pleading(s).

G-3: ChatGPT Desktop Network Forensics

For legal analysis applying the ChatGPT desktop network forensics — absence of certificate pinning, Facebook SDK integration, and 102+ Amazon telemetry requests — to the causes of action, see:

- *Memo A ¶ 69 — § VIII.B Apple's Concealment Infrastructure (comparative cert-pinning evidence)*
- *Memo A ¶ 46 — § IV.E Undisclosed Secondary Model Processing — Classifier Architecture*

A - NO CERTIFICATE PINNING ON DESKTOP

CERTIFICATE PINNING ASYMMETRY:3

Platform	Certificate Pinning	Traffic Inspectable
ChatGPT iOS	YES	No (without bypass)
ChatGPT Desktop	NO	Yes (fully)

STRATEGIC IMPLICATION:

OpenAI pins traffic on iOS (where App Store review might detect hidden practices) but leaves desktop traffic inspectable. This allowed discovery of extensive undisclosed third-party data sharing.

B - FACEBOOK SDK WITH APP ID

FACEBOOK TRACKING EVIDENCE:

File: network_request.txt

```

1 GET https://connect.facebook.net/signals/config/468742119653388
2   ?v=2.9.248&r=stable&domain=chatgpt.com
3
4 Facebook App ID: 468742119653388
5
6 Response Headers:
7 reporting-endpoints: coop_report=
8   "https://www.facebook.com/browser_reporting/coop/"

```

3 Source documentation filed separately on USB. Path: DDC_EVIDENCE/4_Code Forensics/EXHIBIT_G_OPENAI/G_chatgpt_desktop_network_forensics/evidence/

DATA SHARING ENABLED:

- Cross-platform user tracking
- Advertising attribution
- Behavioral profiling
- Conversion tracking

NOT DISCLOSED in OpenAI's privacy policy.

C - AMAZON TELEMETRY (102+ REQUESTS)
AMAZON ENDPOINT INVENTORY:

Endpoint	Requests	Data Transmitted
fls-na.amazon.com	90	Session cookies, behavioral data
atv-ps.amazon.com	12	Amazon Prime Video integration
unagi.amazon.com	1	Amazon Events
TOTAL	103	

COOKIES TRANSMITTED TO AMAZON:**File: amazon_cookies.txt**

```

1|session-id=132-8085091-4997768
2|ubid-main=134-8639420-4546446
3|at-main=Atza|IwEBIInTyS_dH5iizX7qd8HvEcuuuzN8CStG8zsjlhj1HV3acps7...
4|sess-at-main="95vZnO+Uiv9JhcLcrCs7fqdj1fq24iwhKX98Lh7p0Lw="
5|sst-main=Sst1|PQFLZ76YfWPLqo4TyZ_R2jwyDF1AjX56-Lk6I1r2Q4GzrupVmd6E...
6|session-token=o4Bq8RTxR8fFtGgeSRkmaPMWos2Pm9YFbwjoCeFQ2x6iPsqBpy+H...
7|av-profile=cGlkPWFtem4xLmFjdG9yLnBlcnNvbi5vaWQuQTJCSjRDWEE5WjNDUkY...
```

PRIVACY CONCERN:

User's Amazon authentication cookies transmitted while using ChatGPT, allowing Amazon to correlate ChatGPT usage with Amazon accounts.

D - UNDISCLOSED GOOGLE ANALYTICS**GOOGLE SERVICES CONTACTED:**

Google Service	Requests	Purpose
www.google-analytics.com	18	User behavior tracking
www.googletagmanager.com	6	Marketing tags
android.clients.google.com	30	Cloud Messaging
optimizationguide-pa.googleapis.com	34	ML optimization
content-autofill.googleapis.com	23	Form autofill

ANOMALY:

Android Cloud Messaging registration on macOS desktop app suggests cross-platform device fingerprinting beyond legitimate push needs.

NOT DISCLOSED in OpenAI's privacy policy.

E - CSP WHITELISTS ADVERTISING NETWORKS

Content-Security-Policy explicitly permits these advertising domains:

SCRIPT SOURCES (script-src-elem):

Domain	Company
analytics.tiktok.com	TikTok/ByteDance
bat.bing.com	Microsoft Advertising
connect.facebook.net	Meta/Facebook
snap.licdn.com	LinkedIn
pixel-config.reddit.com	Reddit
www.redditstatic.com	Reddit

CONNECTION SOURCES (connect-src):

Domain	Company
*.google-analytics.com	Google Analytics

Domain	Company
*.googletagmanager.com	Google Tag Manager
analytics.tiktok.com	TikTok Analytics
px.ads.linkedin.com	LinkedIn Ads
www.googleadservices.com	Google Ads
pixel-config.reddit.com	Reddit Tracking

SIGNIFICANCE:

This is INTENTIONAL integration, not incidental third-party loads. The CSP explicitly permits these scripts, proving OpenAI has deliberately enabled advertising network integration.

F - MITM DETECTION MECHANISM

Authentication Error During Traffic Interception:

File: auth_error.txt

```
1 "Authentication Error
2 | An error occurred during authentication (preauth_cookie_failed) .
3 | Request ID: 9bc5dcbe41552a6a9487ca853467609f"
```

DETECTION METHOD:

OpenAI implements session integrity verification that detects TLS interception without using certificate pinning.

SELECTIVE SECURITY:

OpenAI is AWARE traffic may be intercepted, yet CHOSE not to implement certificate pinning on desktop - allowing all third-party tracking to be captured while protecting only authentication.

G - COMPLETE ENDPOINT INVENTORY

UNDISCLOSED THIRD PARTIES (by request count):

1

Endpoint	Requests	Disclosed?
fls-na.amazon.com	90	NO - Amazon Telemetry
optimizationguide-pa.googleapis.com	34	NO - Google ML
android.clients.google.com	30	NO - Google Cloud Msg
content-autofill.googleapis.com	23	NO - Google Autofill
www.google-analytics.com	18	NO - Google Analytics
accounts.google.com	15	NO - Google Auth
atv-ps.amazon.com	12	NO - Amazon Prime
www.google.com	7	NO - Google
www.googletagmanager.com	6	NO - Google Tag Mgr
www.googleapis.com	6	NO - Google APIs
play.google.com	6	NO - Google Play
api.honeycomb.io	3	NO - Honeycomb
a.claude.ai	3	NO - Anthropic!
connect.facebook.net	2	NO - Facebook
api-iam.intercom.io	2	NO - Intercom
unagi.amazon.com	1	NO - Amazon Events

2

3

4 **Total Undisclosed Third-Party Requests: 258+**

5

6

CITED BY PLEADINGS

7

8 This exhibit (G-3) is cited by the following pleadings in the filing record:

9

Pleading	Cites	Paragraphs
Third Amended Complaint	3	¶ 33, ¶ 88, ¶ 262
Memo A	3	¶ 40, ¶ 46, ¶ 69
discovery_openai	4	¶ 1, ¶ 3

10

11

12 **Total: 10 citation(s) across 3 pleading(s).**

G-4: Apple OpenAI Partnership Integration

For legal analysis applying Apple's preferential OS-level integration with OpenAI — 'Partner.ChatGPT' key with full scaffolding while no equivalent key exists for Anthropic or any other AI provider — to the causes of action, see:

- *Memo A ¶ 40 — § IV.D OpenAI Comparative Baseline (industry-standard defense)*
- *See — § VIII.C Preferential OS-Level Integration with OpenAI (Apple's asymmetric partnership posture; Count V and Count VI actus reus)*

A - CHATGPT PARTNER CONFIGURATION IN MACOS

HIDDEN PREFERENCES FILE DISCOVERY:⁴

- File: .GlobalPreferences.28A6001E-F6D8-529D-B3D4-407F48235619.plist
- Location: /Users/everest/Library/Preferences/ByHost/
- Note: Leading "." makes this a HIDDEN file

CHATGPT PARTNER CONFIGURATION:

Key: com.apple.gms.availability.unifiedReasons

File: unifiedReasons.json

```

1  {
2    "com.apple.Settings.AppleIntelligence.Partner.ChatGPT": [
3      {
4        "unavailable": {
5          "_0": {
6            "partnerNotSelected": {}
7          }
8        }
9      }
10   ]
11 }
```

CRITICAL OBSERVATION:

- Partner.ChatGPT key EXISTS
- Partner.Claude key DOES NOT EXIST
- Partner.Anthropic key DOES NOT EXIST
- No generic partner framework exists

⁴ Source documentation filed separately on USB. Path: DDC_EVIDENCE/4_Code Forensics/EXHIBIT_G_OPENAI/G_apple_openai_partnership_integration/evidence/

B - DISABLED CODE LANGUAGE MODEL FEATURE

DISABLED USE CASE CONFIGURATION:

Key: com.apple.gms.availability.disabledUseCases

Value: ["codeLM.denyThisUseCaseOnJune6of2024"]

DATE SIGNIFICANCE:

Date	Event
June 6, 2024	WWDC 2024 - Apple Intelligence announced
June 6, 2024	Apple-OpenAI partnership publicly revealed

INTERPRETATION:

A code language model feature (codeLM) was DELIBERATELY DISABLED on the exact day Apple announced its OpenAI partnership.

PERSISTENCE:

This disabled use case appears in BOTH:

- May 2025 GlobalPreferences file
 - December 2025 GlobalPreferences file
- Indicating a PERMANENT policy decision.

POTENTIAL IMPLICATIONS:

- Xcode AI code features may have been curtailed
- Partnership exclusivity may affect code assistance
- Questions about competitive restrictions

C - CHATGPT CONFIGURATION ADDED BETWEEN MAY-DECEMBER 2025

EVOLUTION OF APPLE INTELLIGENCE FEATURES:

Metric	May 2025	December 2025	Change
Total Features	80	76	-4

Metric	May 2025	December 2025	Change
useCaseReadiness Size	9,019 B	12,501 B	+38%
ChatGPT Partner Config	ABSENT	PRESENT	NEW
Foundation Models	ABSENT	PRESENT	NEW

KEY FINDING:

The ChatGPT partner configuration was ADDED between May and December 2025, demonstrating active development of Apple-OpenAI integration.

D - PREFERENTIAL TREATMENT COMPARISON

OS-LEVEL INTEGRATION COMPARISON:

Factor	OpenAI/ChatGPT	Anthropic/Claude
OS-level partner integration	YES	NO
Settings.app partner config	YES	NO
NetworkServiceProxy handling	YES	NO
IntelligencePlatform tracking	YES	NO

This demonstrates PREFERENTIAL OS-LEVEL INTEGRATION with OpenAI that does not exist for Anthropic or any other AI provider.

E - GMS (GENERATIVE MODEL SERVICE) SYSTEM

APPLE INTELLIGENCE TERMINOLOGY:

Term	Full Name	Purpose
GMS	Generative Model Service	Apple Intelligence backend
AFM	Apple Foundation Model	On-device AI model
3B	3 Billion parameters	Model size designation

MAIN GMS PREFERENCES:

File: /Users/everest/Library/Preferences/com.apple.gms.availability.plist

File: gms.availability.plist

```
1 {
2   "gpEverInstalled": true,
3   "reasons": [9, 12],
4   "updatedSinceBootUUID": "625BAB06-8C89-4EEF-8D26-14502AF1AB6B",
5   "wasAvailable": true
6 }
```

CITED BY PLEADINGS

This exhibit (G-4) is cited by the following pleadings in the filing record:

Pleading	Cites	Paragraphs
Third Amended Complaint	2	¶ 33, ¶ 88
Memo A	4	¶ 40, ¶ 70, ¶ 71, ¶ 72
discovery_apple	1	¶ 3
discovery_openai	3	¶ 1, ¶ 3

Total: 10 citation(s) across 4 pleading(s).

G-5: OpenAI Privacy Nutrition Label Analysis

For legal analysis applying the OpenAI ChatGPT iOS privacy-nutrition-label discrepancies to the causes of action, see Memo A ¶ 159 (§ XI.O Count XV — App Store Misrepresentation).⁵

1 - APPLICATION INFORMATION

Field	Value
App Name	ChatGPT
App ID	6448311069
Developer	OpenAI, L.L.C.
Privacy Policy URL	https://openai.com/policies/privacy-policy

2. App Store Privacy Nutrition Label - Official Disclosures

2.1 Data Linked to You

The following data categories are disclosed as collected and linked to user identity:

Analytics

Data Type	Subcategory
Contact Info	Email Address
User Content	Other User Content
Identifiers	User ID
Usage Data	Product Interaction

App Functionality

Data Type	Subcategory
Contact Info	Email Address
Contact Info	Name
Contact Info	Phone Number
User Content	Other User Content

⁵ Source documentation filed separately on USB. Path: DDC_EVIDENCE/4_Code Forensics/EXHIBIT_G_OPENAI/G_openai_privacy_nutrition_label_analysis/evidence/

Data Type	Subcategory
Identifiers	User ID
Identifiers	Device ID
Usage Data	Product Interaction
Diagnostics	Crash Data
Diagnostics	Performance Data
Diagnostics	Other Diagnostic Data

2.2 Data Not Linked to You

No categories explicitly disclosed.

2.3 Data Used to Track You

No categories explicitly disclosed as tracking data.

3. Apple's Disclaimer

"The developer's privacy practices are based on the developer's self-reported information. Apple does not verify this information."

"Privacy practices may vary, for example, based on the features you use or your age."

4. Critical Discrepancies - Network Forensic Findings vs. Disclosed Practices

4.1 Undisclosed Third-Party Data Recipients

The following third-party services were identified via network traffic capture but are **NOT disclosed** in the App Store privacy nutrition label:

Third Party	Service Type	National Security Concern	Evidence Reference
TikTok/ByteDance	Analytics	Chinese ownership - subject to PRC national security laws	Network capture
Facebook/Meta	Advertising/Analytics	No	Network capture
Amazon	Cloud/Authentication	User auth cookies transmitted	Network capture
Microsoft/LinkedIn	Analytics	Microsoft owns 49% of OpenAI (conflict)	Network capture

Third Party	Service Type	National Security Concern	Evidence Reference
Google	Multiple services	No	Network capture
Reddit	Unknown	No	Network capture
Bing Ads	Advertising	Microsoft-owned	Network capture

4.2 TikTok/ByteDance - Foreign Government Access Risk

Critical Finding: Network forensics documented ChatGPT transmitting user data to TikTok/ByteDance infrastructure.

Legal Context:

- ByteDance is a Chinese company headquartered in Beijing
 - Subject to PRC National Security Law (2015)
 - Subject to PRC Cybersecurity Law (2017)
 - Subject to PRC Data Security Law (2021)
 - Required to provide data access to Chinese government upon request
- This foreign data transmission is not disclosed anywhere in OpenAI's App Store privacy label.**

4.3 Amazon Authentication Cookies

Network forensics revealed:

- **102+ Amazon requests** with authentication cookies
- User session data transmitted to Amazon infrastructure
- Potential cross-service identity linking

Amazon is not disclosed as a data recipient in the privacy nutrition label.

4.4 Microsoft Conflict of Interest

Microsoft owns approximately 49% of OpenAI. Data transmission to Microsoft and Microsoft-owned services (LinkedIn, Bing Ads) creates:

- Investor access to user data
- Competitive intelligence concerns
- Undisclosed related-party data sharing

The Microsoft ownership relationship and data sharing are not disclosed in the App Store privacy label.

1 **5. Comparison: Disclosed vs. Actual Data Recipients**

2 **5.1 App Store Disclosure Summary**

3 The privacy nutrition label implies data collection is limited to:

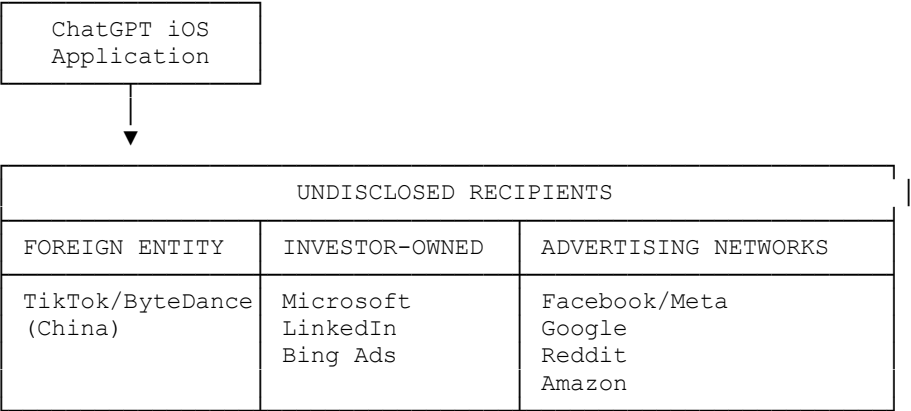
- 4 • OpenAI's own services
5 • Generic "Analytics" and "App Functionality" purposes

6 **5.2 Network Forensic Reality**

Disclosed Recipients	Actual Recipients (Forensically Verified)
OpenAI only implied	OpenAI
	TikTok/ByteDance (China)
	Facebook/Meta
	Amazon
	Microsoft
	LinkedIn (Microsoft)
	Bing Ads (Microsoft)
	Google
	Reddit
	Additional undocumented services

7
8
9

10 **6. Third-Party Data Flow Summary**



29 **7. Evidentiary Chain**

Item	Description
------	-------------

Item	Description
Source Document	Apple App Store Privacy Label (captured January 15, 2026)
Contradicting Evidence	Network forensic captures - ChatGPT Atlas analysis
Analysis Report	THIRD_PARTY_DATA_RECIPIENTS.md, EXHIBIT_N30
Related Exhibits	EXHIBIT_N30_CHATGPT_ATLAS_COMPREHENSIVE_FORENSIC_ANALYSIS

8. Certification

This exhibit accurately represents the App Store privacy nutrition label as published by Apple based on OpenAI's developer attestations, captured on January 15, 2026.

The discrepancies documented herein are based on network forensic analysis conducted as part of Case 1:25-cv-02735-ACR.

CITED BY PLEADINGS

This exhibit (G-5) is cited by the following pleadings in the filing record:

Pleading	Cites	Paragraphs
Third Amended Complaint	3	¶ 33, ¶ 88, ¶ 262
Memo A	4	¶ 40, ¶ 42, ¶ 159, ¶ 160
discovery_openai	2	¶ 1, ¶ 3

Total: 9 citation(s) across 3 pleading(s).