APP STORE PRIVACY LABELS MAPPING

RecallScope Pty LTD
Unit 7, 2 Elonera Street
Rydalmere, New South Wales 2116
Australia

Document Version: 1.0
Last Updated: November 12, 2025
Purpose: App Store Connect Privacy Section Configuration

1. INTRODUCTION AND COMPLIANCE FRAMEWORK

This document provides comprehensive mapping of RecallScope's data collection practices to Apple's App Store Privacy Labels framework (also known as "Privacy Nutrition Labels"), as required for App Store submission under Apple's App Store Review Guidelines Section 5.1.2.

Apple's Privacy Labels framework mandates that developers disclose all data collected by their applications, including data collected by integrated third-party SDKs, and categorise such data according to three principal classifications: (a) Data Used to Track You; (b) Data Linked to You; and (c) Data Not Linked to You. This disclosure requirement became mandatory for all new app submissions and updates beginning December 8, 2020.

Since May 2024, Apple additionally requires submission of a Privacy Manifest file (PrivacyInfo.xcprivacy) declaring collected data types, API usage justifications, and third-party SDK disclosures. This document addresses both the App Store Connect web form disclosures and Privacy Manifest requirements.

2. DEFINITIONS OF KEY TERMS

Data Collection. Under Apple's framework, "collect" means transmitting data off the device in a manner that allows the developer or third-party partners to access such data for a period longer than necessary to service the transmitted request in real time. Ephemeral data processed solely for immediate request fulfillment (e.g., API calls where responses are not stored) does not constitute collection.

Tracking. "Tracking" refers to linking user or device data collected from your app with user or device data collected from other companies' apps, websites, or offline properties for targeted advertising or advertising measurement purposes. Tracking also includes sharing user or device data with data brokers. Apps that engage in tracking must implement App Tracking Transparency ("ATT") and request explicit user permission through the NSUserTrackingUsageDescription prompt.

Data Linked to You. Data is "linked to you" when it is connected to the user's identity, including name, email address, Account identifier, device identifier associated with the user, or any other information that identifies or can reasonably be used to identify the user or their device. This includes data linked to user profiles across sessions.

Data Not Linked to You. Data that is collected in a manner that cannot reasonably be linked back to a specific user or device identity falls into this category. This typically includes aggregated analytics data or anonymous crash reports where identifiers have been stripped.

3. RECALLSCOPE DATA COLLECTION SUMMARY

RecallScope collects the following categories of data through first-party mechanisms and third-party SDKs integrated into the Application: Contact Information (email addresses via authentication); Identifiers (User IDs, Device IDs, advertising identifiers); Usage Data (product

interactions, search history, scans); Diagnostics (crash data, performance data); and Purchases (subscription history).

The following third-party SDKs integrated into RecallScope collect or process user data and must be disclosed:

- **Firebase Suite** (Google LLC): Authentication, Firestore, Cloud Functions, Cloud Messaging, Analytics, Crashlytics
- **Google AdMob** (Google LLC): Advertising delivery and measurement
- **AppsFlyer Ltd.**: Attribution analytics
- **Apphud Inc.**: Subscription management

4. DATA USED TO TRACK YOU

This section identifies data collected for tracking purposes, requiring App Tracking Transparency implementation.

Tracking Status: NO

RecallScope **does not** engage in tracking as defined by Apple. Specifically:

- RecallScope does not link user or device data collected from the Application with data collected from other companies' apps, websites, or offline properties for targeted advertising purposes.
- RecallScope does not share user data with data brokers.
- AdMob advertisements are served in non-personalized mode by default; personalized advertising requires explicit opt-in consent obtained through in-app privacy settings, independent of ATT.
- AppsFlyer attribution data is used solely for measuring RecallScope's own marketing campaign performance and is not shared with third parties for cross-app tracking.

Consequence: RecallScope is **not required** to display the App Tracking Transparency prompt and should answer "No" to the question "Does this app use data for tracking purposes?" in App Store Connect.

Important Note: If RecallScope enables personalized advertising through AdMob or shares advertising identifiers with third parties for cross-context behavioral advertising, tracking disclosure becomes mandatory and ATT implementation is required.

5. DATA LINKED TO YOU

Data in this category is connected to the user's identity and must be disclosed with associated purposes.

5.1 Contact Info

Email Address

Collected: Yes
Linked to User: Yes
Used for Tracking: No
Purposes: App Functionality (authentication), Analytics (optional weekly digest delivery)
Source: Apple Sign-In, Google Sign-In

5.2 Identifiers

User ID

Collected: Yes
Linked to User: Yes
Used for Tracking: No
Purposes: App Functionality (account management, Watchlist synchronization, subscription entitlement verification)
Source: Firebase Authentication, Apphud

Device ID

Collected: Yes
Linked to User: Yes (when associated with authenticated Account)
Used for Tracking: No
Purposes: App Functionality (device registration for push notifications), Analytics (usage tracking across sessions), Product Personalisation (device-specific settings)
Source: Firebase Cloud Messaging, Firebase Analytics

Advertising ID (IDFA/AAID)

Collected: Conditionally (only for free-tier users who have not subscribed)
Linked to User: No (collected but not linked to user identity)
Used for Tracking: No (non-personalized ads only by default)
Purposes: Third-Party Advertising (contextual ad delivery through AdMob)
Source: Google AdMob

Note: If users opt into personalized advertising, IDFA becomes linked to user and tracking disclosure may be required.

5.3 Purchases

Purchase History

Collected: Yes
Linked to User: Yes
Used for Tracking: No
Purposes: App Functionality (subscription entitlement management, feature access control), Analytics (subscription conversion tracking)
Source: App Store StoreKit, Apphud

5.4 Usage Data

Product Interaction

Collected: Yes
Linked to User: Yes
Used for Tracking: No
Purposes: Analytics (feature usage measurement, engagement tracking), App Functionality (Watchlist management), Product Personalisation (notification preferences)
Source: Firebase Analytics, first-party event logging

Examples: App launches, screen views, Watchlist additions, notification interactions, search queries, barcode scans.

5.5 Search History

Search History

Collected: Yes
Linked to User: Yes
Used for Tracking: No
Purposes: App Functionality (recall matching, search suggestions), Analytics (search pattern analysis for Service improvement), Product Personalisation (recent searches)
Source: First-party search functionality, Firebase Firestore

5.6 Diagnostics

Crash Data

Collected: Yes
Linked to User: Yes (User ID included in crash reports for authenticated users)
Used for Tracking: No
Purposes: App Functionality (bug identification and resolution)
Source: Firebase Crashlytics

Performance Data

Collected: Yes
Linked to User: Yes
Used for Tracking: No
Purposes: Analytics (performance monitoring, optimization), App Functionality (identifying slow operations)
Source: Firebase Performance Monitoring, Firebase Analytics

Other Diagnostic Data

Collected: Yes
Linked to User: Yes
Used for Tracking: No
Purposes: App Functionality (error logging, debugging)
Source: Firebase Crashlytics, custom logging

6. DATA NOT LINKED TO YOU

Data in this category is collected in anonymised or aggregated form not reasonably linkable to user identity.

6.1 Location (Coarse)

Coarse Location

Collected: Yes (inferred from IP address)
Linked to User: No
Used for Tracking: No
Purposes: App Functionality (jurisdiction-appropriate recall display), Analytics (geographic usage patterns)
Source: Firebase Analytics, server-side IP geolocation

Note: RecallScope does not collect precise location data. Users manually select jurisdictions of interest.

6.2 Identifiers (Anonymous Analytics)

Device ID (Aggregated Analytics)

Collected: Yes
Linked to User: No (aggregated in Firebase Analytics after 14 months)

Used for Tracking: No
Purposes: Analytics (aggregated usage statistics)
Source: Firebase Analytics

7. DATA NOT COLLECTED

The following data types are **not collected** by RecallScope and should be marked as "No" in App Store Connect:

- Health & Fitness data
- Financial Info (payment credentials; handled exclusively by App Store)
- Precise Location
- Sensitive Info (racial, ethnic, sexual orientation, religious, political, biometric data)
- Contacts (user's contact list)
- Photos or Videos
- Audio Data
- Gameplay Content
- Customer Support data (unless voluntarily provided in support requests, which qualifies for optional disclosure)
- Browsing History
- Environment Scanning
- Body (hands, head movement)

8. OPTIONAL DISCLOSURE EXEMPTIONS

Certain data collection may qualify for optional disclosure under Apple's criteria. RecallScope evaluates the following:

Customer Support Communications. Data voluntarily provided by users through support requests (via support@recallscope.com) qualifies for optional disclosure where: (a) collection is infrequent and not part of primary app functionality; (b) user affirmatively chooses to provide data each time; (c) it is clear what data is collected; and (d) data is not used for tracking.

Recommendation: While technically optional, RecallScope should disclose customer support data collection to maintain transparency and avoid potential App Store rejection.

9. PRIVACY MANIFEST REQUIREMENTS

RecallScope's Privacy Manifest file (PrivacyInfo.xcprivacy) must declare the following:

NSPrivacyCollectedDataTypes: All data types listed in Sections 5 and 6 above, with the following attributes for each:

- NSPrivacyCollectedDataType: Data type code (e.g., NSPrivacyCollectedDataTypeEmailAddress)
- NSPrivacyCollectedDataTypeLinked: Boolean indicating linked status
- NSPrivacyCollectedDataTypeTracking: Boolean indicating tracking usage (false for all RecallScope data)

- NSPrivacyCollectedDataTypePurposes: Array of purpose codes (e.g., NSPrivacyCollectedDataTypePurposeAppFunctionality)

NSPrivacyTrackingDomains: Empty array (RecallScope does not engage in tracking).

NSPrivacyAccessedAPITypes: Declaration of required reason APIs (e.g., UserDefaults access for storing preferences, system boot time access for diagnostics) with corresponding reason codes.

10. APP STORE CONNECT CONFIGURATION SUMMARY

When completing the App Privacy questionnaire in App Store Connect, RecallScope should provide the following answers:

Does this app collect data from this app? Yes

Do you or your third-party partners use data from this app for tracking purposes? No

Data Types to Declare:

- Contact Info: Email Address
- Identifiers: User ID, Device ID
- Purchases: Purchase History
- Usage Data: Product Interaction, Search History
- Diagnostics: Crash Data, Performance Data, Other Diagnostic Data
- Location: Coarse Location (Data Not Linked to You)

For each data type, select applicable purposes from: App Functionality, Analytics, Product Personalisation, Third-Party Advertising (AdMob only).

11. ONGOING MAINTENANCE OBLIGATIONS

Apple requires that privacy disclosures be kept accurate and up to date. RecallScope must update App Store Connect privacy responses whenever:

- New SDKs are integrated that collect user data
- Data collection practices change (e.g., enabling personalised advertising, collecting new data types)
- Third-party SDK privacy practices change materially

Updates may be made without submitting a new app version, though updating the Privacy Manifest requires an app update submission.