Coordinated Security & Privacy Disclosure, Final Report

Snapchat for Android (com.snapchat.android)

Social media and messaging platform, 750M+ monthly active users

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – NINETY DAYS, ONE FINDING DISPUTED, SIX UNADDRESSED

Target	Snap Inc., Santa Monica, California, US / Snap Group Limited, London, UK (EU/UK GDPR entity)
Product audited	Snapchat for Android, com.snapchat.android, versionName 14.11.0.49, versionCode 295722
Disclosure reference	RFI-IRFOS Snapchat 2026-06-20, Zendesk ticket N2LX1Z, later #274553938
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (SC-01, CVSS v4.0 8.2 High) / SC-03 scores highest of the set at 8.7 High
SHA-256 (base APK)	`eba03ac00691c3e02ff67a685285480785d86e98f491368e053ddf155b29c2d0`

rfi.irfos@gmail.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

Snapchat markets itself on the promise that snaps and chats disappear, a claim central to its brand, its consumer-facing representations, and the 2014 FTC consent order that specifically concerned this same promise. RFI-IRFOS's root level static analysis of the production Android build (version 14.11.0.49, 87,316 smali classes) found that the app's own backup agent, purpose-built and named for Snapchat's Fidelius end-to-end encryption system, registers two SharedPreference archives for inclusion in Android's Backup Service with android:allowBackup="true". Separately, the on-device SQLite schema stores per-contact Fidelius encryption keys in a fideliusKeys BLOB column. Six further findings span an unscoped ACCESS_BACKGROUND_LOCATION grant, a shake-triggered full-screen capture path that can record private content, hardcoded Facebook and Google API credentials, a Digital Services Act illegal-content reporting mechanism implemented for advertisements only, exposed internal Snapchat infrastructure URLs, and an unclear consent basis for a generative-AI feature that processes facial biometric data.

RFI-IRFOS notified security@snap.com on 20 June 2026 and copied the Austrian DSB, the EDPB, the UK ICO, CERT.at, and Coimisiun na Mean, Ireland's Digital Services Coordinator for Snap under the DSA. Coimisiun na Mean initially responded that it could not act on a complaint from a non-Irish party; RTR, Austria's own Digital Services Coordinator, formally transmitted the case under the DSA's Art. 53/57 cross-border cooperation mechanism on 12 August 2026, after which Coimisiun na Mean's own case CAS-09535, opened 29 June 2026, proceeded on record. Snap itself gave only an automated acknowledgment for 88 days despite five written follow-ups.

On 16 September 2026, three days before the embargo, Snap's DSA Team gave RFI-IRFOS its only specific, falsifiable technical response of the entire correspondence: that the two backed-up SharedPreference archives do not, in fact, contain the cited fideliusKeys database column or message payloads. RFI-IRFOS credits this as the first genuine technical engagement in the case, and this report states plainly what that response does and does not settle. It does not answer the separate question RFI-IRFOS put in writing on 4 September 2026 and repeated on 16 September 2026: whether Snap Inc. retains any server side capability to decrypt Fidelius protected content, for any content class. That question remains open. The other six findings received no response of any kind.

Scope: Static, root level analysis of the publicly downloaded Snapchat for Android production APK only. No Snap servers, accounts, or backend infrastructure were accessed or tested. No live Android Backup Service capture or restore was performed; the backup-content dispute described in this report reflects that limitation on both sides, RFI-IRFOS's original inference from code and naming conventions, and Snap's rebuttal, neither independently confirmed by dynamic testing in this cycle.

Disposition

Reported 20 June 2026 to security@snap.com, with the Austrian DSB, EDPS, ICO, CERT.at, and Coimisiun na Mean bcc'd. Coimisiun na Mean (Ireland's DSA Digital Services Coordinator for Snap) initially declined to act on a non-Irish complainant; RTR, Austria's own Digital Services Coordinator, formally transmitted the case under DSA Art. 53/57 cooperation on 12 August 2026, and Coimisiun na Mean opened formal case CAS-09535 on 29 June 2026. Snap itself gave no reply beyond an automated ticket acknowledgment for 88 days. On 16 September 2026, three days before embargo, Snap's DSA Team gave the only specific technical response of the entire correspondence, disputing the mechanism (not the existence) of SC-01. The six other findings, including the ACCESS_BACKGROUND_LOCATION finding that scores highest under CVSS v4.0 of the whole set, received no reply of any kind.

ID	Severity	Title
SC-01	CRITICAL	Fidelius encryption keys registered for backup to Google; "disappearing" messages promise contradicted
SC-02	HIGH	Internal development infrastructure URLs exposed in production APK
SC-03	HIGH	ACCESS_BACKGROUND_LOCATION not scoped to active location-sharing sessions
SC-04	HIGH	shake2report bug-reporting tool can capture private snap or DM content via MediaProjection
SC-05	HIGH	Facebook App ID, Facebook client token, and Google API key hardcoded in release build
SC-06	MEDIUM	DSA illegal-content reporting mechanism implemented for advertisements only
SC-07	MEDIUM	"My Selfie" / Dreams generative-AI feature processes facial biometric data under an unclear consent basis

Subject & Operator Analysis

Snap Inc. (Santa Monica, California) operates Snapchat globally; Snap Group Limited (London, UK) is the entity of record for EU/UK GDPR purposes, making the UK Information Commissioner's Office the lead supervisory authority for EU/EEA processing via the post-Brexit UK GDPR adequacy framework, with the EDPB coordinating EU-level enforcement. Snap publicly reports over 750 million monthly active users globally and approximately 100 million in the EU, placing it within Very Large Online Platform scope under the Digital Services Act, for which Ireland's Coimisiun na Mean is the Digital Services Coordinator. Snap and the FTC entered a consent order in 2014 specifically concerning misrepresentations about the persistence of "disappearing" Snapchat content, the same underlying claim SC-01 in this report concerns.

Architecture & Data Flow

- Fidelius: on-device end-to-end encryption for Snap and Chat content, keys stored per-contact in a local SQLite BLOB column, correctly enabled by default (isFideliusReady = 1).
- MushroomBackupAgent: a dedicated backup agent, named for the Fidelius system, registers two SharedPreference archives with Android Backup Service under a global allowBackup="true" flag.
- SnapMap / Live Location: background location pipeline gated by ACCESS_BACKGROUND_LOCATION plus FOREGROUND_SERVICE_LOCATION, with a working Ghost Mode opt-out but no session-scoped permission lifecycle found in static analysis.
- shake2report: an internal bug-reporting tool using MediaProjectionManager to capture the full device screen on a shake gesture, routed to Snap's internal crash/bug pipeline.
- My Selfie / Dreams: generative-AI imagery from user and friend facial data, gated by a default-off per-friend permission flag in the same Friend table that stores Fidelius key material.

Findings

SC-01: Fidelius encryption keys registered for backup to Google; "disappearing" messages promise contradicted

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.2

android:allowBackup="true" with android:backupAgent="com.snap.backup.api.MushroomBackupAgent", which registers SharedPreferencesBackupHelper entries named fidelius_encrypted_backup_records and fidelius_device_user_records for Android Backup Service. The Friend table schema separately stores fideliusKeys BLOB, per-contact end-to-end encryption keys, in plaintext SQLite.

```
; MushroomBackupAgent.smali:
new-instance v0, Landroid/app/backup/SharedPreferencesBackupHelper;
const-string v1, "fidelius_encrypted_backup_records"
const-string v2, "fidelius_device_user_records"
invoke-virtual {p0, v1, v0}, ...BackupAgentHelper;->addHelper(...)

; Friend table, GYf.smali:
isFideliusReady INTEGER NOT NULL DEFAULT 1,
fideliusKeys BLOB,   -- per-contact E2E encryption keys
```

Snap's response, 16 September 2026

Snap DSA Team, verbatim: "the backup agent identified in your report is configured to export limited Fidelius-related preference archives. Those archives do not include the cited Friend database field or Snap or Chat message payloads. If you have reproducible evidence showing that an Android backup contains the cited database field or message payloads... you may provide it for review. Otherwise, our review of SC-01 is complete."

This is a narrow, specific, and credible rebuttal: it disputes the inferential link between the backup agent's two named SharedPreference archives and the separate SQLite fideliusKeys column, not the existence of the backup agent or its naming. RFI-IRFOS did not perform a live device backup-and-restore capture to confirm the byte level contents of the actual Android Backup Service payload, the same static-only discipline this programme applies to every target; the original finding's link between the two data stores was drawn from naming convention and co-location in the same binary, not a captured backup archive. Neither RFI-IRFOS's original inference nor Snap's rebuttal has been independently confirmed by dynamic testing in this cycle. What Snap's 16 September reply does not address is the separate, explicitly posed question of 4 September 2026, repeated the same day as their reply: whether Snap Inc. retains any server side capability to decrypt Fidelius protected content, for any content class. A backup-content dispute and a server side decryption capability question are two different claims about two different failure modes, and only the first received a specific answer.

Impact: If confirmed, key material backed up outside the two-endpoint model a genuine E2EE design requires would let anyone with access to the account's Google backup, including via legal process served on Google rather than Snap, recover content its users were told had

disappeared, a subset of Snap's own userbase being minors sharing sensitive content under that specific assumption.

Fix: Set android:allowBackup="false" or exclude all Fidelius-related SharedPreference archives from the backup helper. Independently of this dispute, publish a reproducible test (a device backup capture and inspection) settling what the archives actually contain, and answer in writing whether Snap Inc. holds any server side Fidelius decryption capability.

SC-02: Internal development infrastructure URLs exposed in production APK

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:L/SI:N/SA:N, 6.9

SQL schema strings embedded in the APK carry developer comments linking to github.sc-corp.net (internal GitHub Enterprise), jira.sc-corp.net, and an internal Google Drive document, including the file path of Snapchat's own abuse-reporting protobuf schema.

```
https://github.sc-corp.net/Snapchat/pb_schema/.../proto/abuse/support/in_app_warning.
    proto
https://github.sc-corp.net/Snapchat/android/pull/146638#discussion_r1914549
https://jira.sc-corp.net/browse/CP-10972
https://jira.sc-corp.net/browse/DATP-43544
https://drive.google.com/a/snapchat.com/open?id=1
    yrScy1HabK3S5ix86TQUZ0_SKPgRNOjZ0xjXOZFbm_U
```

No response was received naming this finding. The CVSS score is qualitatively lower than the report's own HIGH label because no direct confidentiality, integrity, or availability impact on Snapchat's app or user data was demonstrated, the exposure is reconnaissance value against Snap's own internal infrastructure, captured here as a Subsequent System impact. RFI-IRFOS keeps the HIGH label in the narrative severity because the abuse-reporting proto path specifically maps API surface relevant to child-safety and illegal-content handling, a target of particular interest to the same threat actors documented against this platform elsewhere in this report.

Impact: An attacker profiling Snap's internal infrastructure gains a confirmed GitHub Enterprise hostname, repository namespace, Jira project codes, and the specific API surface path for abuse and illegal-content handling.

Fix: Strip SQL string comments via ProGuard/R8 in release builds. Enforce a code-review rule against sc-corp.net or internal Google Workspace URLs surviving minification.

SC-03: ACCESS_BACKGROUND_LOCATION not scoped to active location-sharing sessions

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.7

ACCESS_BACKGROUND_LOCATION plus FOREGROUND_SERVICE_LOCATION permit GPS-precision location collection while the app is backgrounded or the screen is off. Static analysis found no scoping of this permission to an active SnapMap live-sharing session.

No response was received naming this finding. This is the highest CVSS v4.0 score of the entire disclosure, 8.7, above SC-01's 8.2, because continuous precise location is a directly demonstrated confidentiality impact requiring no external precondition, unlike SC-01's requirement that an attacker first hold access to the victim's Google account. Ghost Mode is a genuine, working opt-out (credited under Positive Observations below), but the permission grant itself is not time-boxed to an active sharing session in the code paths examined. For minors, GDPR Art. 8 and the US COPPA Rule (16 CFR Part 312) require verified parental consent for this class of continuous processing, a bar an install-time permission bundle does not meet.

Impact: Continuous background GPS collection outside an active, user-initiated sharing session, including for minor users, without a demonstrated separate consent step beyond the install-time permission grant.

Fix: Request ACCESS_FINE_LOCATION only by default. Escalate to background location solely for the duration of an explicit, user-initiated SnapMap live-sharing session, and auto-revoke on session end.

SC-04: shake2report bug-reporting tool can capture private snap or DM content via MediaProjection

MEDIUM, CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:P/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 5.1

com.snap.shake2report's CaptureScreenService invokes Android's MediaProjectionManager to capture the full device screen. Two further createScreenCaptureIntent() call sites exist in a separate class.

```
; CaptureScreenService.smali:
check-cast v3, Landroid/media/projection/MediaProjectionManager;
invoke-virtual {v3, v0, v2}, ...->getMediaProjection(ILandroid/content/Intent;)...
```

No response was received naming this finding. The CVSS score reflects that the trigger is a local, physical device gesture by the legitimate user rather than a remote attacker (AV:P) and is typically unintentional (UI:P, passive), which lowers the Base score relative to the qualitative HIGH label; the report keeps that label because the resulting capture of ephemeral, sometimes minor-originated content into a persistent internal bug database directly contradicts the same disappearing-content promise at issue in SC-01.

Impact: An accidental device shake while viewing a private snap, an open DM, or a minor's story routes a full-screen capture of that content into Snap's internal bug-reporting pipeline, where it can persist after the original content has expired.

Fix: Apply FLAG_SECURE to all snap viewer and DM activities and block MediaProjection capture while any such activity is in the foreground.

SC-05: Facebook App ID, Facebook client token, and Google API key hardcoded in release build

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:L/SI:L/SA:L, 6.9

res/values/strings.xml embeds facebook_app_id 559927829732067, facebook_client_token af620f69bc26ba9f731132076ff85232, and google_api_key AIzaSyDcMB8X6gNQ9zj05Rbuz5_Zds9V4WQ8nHE, extractable from any downloaded APK.

No response was received naming this finding. Per this programme's standing position, a client-embedded API key is not automatically a secret-exposure finding in itself, the concern is whether server-side restriction (certificate fingerprint, quota scoping) is applied, which cannot be verified from the client binary alone; the finding is scored here as a Subsequent System availability and integrity concern against Facebook's and Google's platforms (quota abuse, calls made under Snapchat's app identity) rather than a direct breach of Snapchat's own systems.

Impact: Anyone extracting the APK can make Facebook Graph API calls under Snapchat's app registration and access the associated Google Cloud project, subject to whatever server-side restriction, unverified from this analysis, Snap has configured.

Fix: Restrict both keys to the production certificate fingerprint. Rotate the Facebook client token. Deliver SDK credentials via Remote Config rather than the shipped APK.

SC-06: DSA illegal-content reporting mechanism implemented for advertisements only

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N, 6.9

Across 87,316 analyzed classes, the only illegal_content implementation found is prefixed snapads_ and scoped to the ad-reporting flow. No equivalent in-app path for snaps, stories, DMs, or Spotlight was located.

```
const-string v10, "snapads_enable_dsa_illegal_content_report"
const-string v10, "snapads_dsa_illegal_content_redirect_url"
const-string v2,  "report_ad_reason_illegal_content"
```

No response was received naming this finding. DSA Art. 16 requires a user-friendly notice-and-action mechanism for illegal content, and Snapchat's own reported scale (publicly stated at approximately 100 million EU monthly active users) places it within Very Large Online Platform obligations under Art. 27 and Art. 33. Snapchat has been named in US DOJ, EU Commission, and national law enforcement material as a platform used for fentanyl sales, CSAM distribution, and sextortion targeting minors; a reporting mechanism that functions for ads but not for the user-generated content those activities actually use is the specific gap this finding documents.

Impact: Users encountering illegal content in snaps, stories, DMs, or Spotlight have no equivalent in-app reporting path to the one available for advertisements, a gap directly relevant to Snap's own DSA systemic-risk obligations.

Fix: Implement a prominent in-app illegal-content reporting flow, compliant with DSA Art. 16(1), accessible from every content surface, not only advertisements.

SC-07: "My Selfie" / Dreams generative-AI feature processes facial biometric data under an unclear consent basis

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9

The Friend table schema includes canUseMySelfie INTEGER NOT NULL DEFAULT 0 and dreamsGenerationPolicy INTEGER, permission flags governing whether a friend's face can be used to generate synthetic AI imagery.

No response was received naming this finding. The default-disabled flag is correct design and is credited under Positive Observations; what static analysis cannot confirm is whether the flow that flips this flag to enabled captures explicit, specific, and revocable consent as GDPR Art. 9(2)(a) requires for biometric data, since generating synthetic imagery from a person's face is processing of special category data regardless of the feature's opt-in default. Under the EU AI Act, synthetic imagery of real identifiable persons also carries a transparency obligation to disclose it as AI-generated.

Impact: A biometric consent flow that does not meet the Art. 9(2)(a) explicit-consent standard, or Dreams-generated imagery not disclosed as AI-generated, would place this feature in violation independent of its correct default-off design.

Fix: Audit the My Selfie consent capture flow against GDPR Art. 9(2)(a) and add an accessible revocation path. Watermark or otherwise flag all Dreams-generated output as AI-generated per EU AI Act transparency requirements.

Impact Analysis

Snapchat's core value proposition to its userbase, including the significant minor population that uses it, is that shared content disappears. Three of the seven findings compound around that single promise from different angles: SC-01 concerns whether content and keys persist via backup, SC-04 concerns whether an accidental gesture can capture and persist content that should have expired, and SC-06 concerns whether the platform's own illegal-content reporting mechanism, the tool meant to catch the worst misuse of that ephemerality, actually reaches the content types where documented criminal misuse (fentanyl sales, CSAM distribution, sextortion of minors, per public DOJ, Europol, and NCMEC material) occurs. None of these are independent bugs; they describe the same structural gap between marketed ephemerality and its actual technical and procedural enforcement, viewed from three different angles.

SC-03's background location finding carries the highest CVSS v4.0 score of the set specifically because it requires no attacker precondition at all: it is a design choice Snap itself controls, affecting every user who grants the permission, including minors whose real-time location during school hours or elsewhere would require verified parental consent under GDPR Art. 8 and COPPA that an install-time bundle does not provide.

Data Protection, Article by Article

Finding	Provision	Concern
SC-01	GDPR Art. 5(1)(b), 5(1)(e), 13(1)(e)	Purpose/storage limitation and disclosure, disputed by Snap on mechanism, not existence, of the backup agent
SC-02	GDPR Art. 32	Internal infrastructure exposure, security-control gap rather than personal-data exposure
SC-03	GDPR Art. 5(1)(c), Art. 6(1)(a); GDPR Art. 8; COPPA (16 CFR Part 312)	Unscoped background location collection; minors require verified parental consent
SC-04	GDPR Art. 5(1)(f), Art. 32	Inadvertent capture of ephemeral private content via an internal tool
SC-05	GDPR Art. 32	Credential hardening, third-party platform risk rather than direct user-data exposure
SC-06	DSA Art. 16, Art. 27, Art. 33	Illegal-content reporting mechanism scoped to ads only, VLOP systemic-risk relevance
SC-07	GDPR Art. 9(2)(a); EU AI Act Annex III	Biometric consent flow for a generative-AI feature not verifiable as explicit from static analysis

Platform Accountability & the DSA

SC-06 sits squarely inside Snap's Digital Services Act obligations. As a platform Snap itself reports at roughly 100 million EU monthly active users, it qualifies as a Very Large Online Platform, carrying Art. 27 algorithmic-transparency and Art. 33 systemic-risk-assessment duties in addition to the baseline Art. 16 notice-and-action requirement every online platform carries regardless of size. A notice-and-action mechanism that functions for advertising complaints but has no demonstrated equivalent for snaps, stories, direct messages, or Spotlight content is a gap in exactly the systemic-risk category, criminal misuse of core platform features, that Art. 33 exists to make platforms assess and address.

Coimisiun na Mean is Ireland's Digital Services Coordinator and the lead DSA authority for Snap. RFI-IRFOS's direct submission (CAS-09535, 29 June 2026) was met with a jurisdictional response: Coimisiun na Mean stated its Online Safety Framework role requires complaints from Irish-located users, and that a non-Irish notifier's submission would need to be transmitted through that notifier's own national Digital Services Coordinator. RFI-IRFOS pursued exactly that channel: RTR, Austria's Digital Services Coordinator, formally transmitted the full evidence submission to Coimisiun na Mean under the DSA's Art. 53/57 cross-border cooperation mechanism on 12 August 2026, after which the case proceeded on record under CAS-09535.

Authority	Role	Status as of publication

Regulatory & Legal Landscape

Authority	Role	Status as of publication
UK ICO	Lead GDPR supervisory authority (Snap Group Limited, London)	Bcc'd at R1; direct submission to case-work@ico.org.uk bounced, no separate ICO web-form submission logged
EDPB	EU-level GDPR coordination	Bcc'd at R1 and on follow-ups
Austrian DSB	Notified party, Austria being RFI-IRFOS's home jurisdiction	Cc'd throughout the correspondence
CERT.at	National CERT, informational copy	Bcc'd/cc'd on R1 and multiple follow-ups
Coimisiun na Mean (Ireland)	DSA Digital Services Coordinator for Snap	Case CAS-09535 opened 29 June 2026; proceeded on record after RTR's formal Art. 53/57 transmission on 12 August 2026
RTR (Austria)	Austria's own DSA Digital Services Coordinator	Formally transmitted the case to Coimisiun na Mean, 12 August 2026
US FTC	Prior enforcement history on the same underlying representation	2014 consent order concerned Snapchat's "disappearing message" claim; not directly petitioned in this cycle

Indicators of Compromise & Reproducible Evidence

- snapchat_base.apk, SHA-256 eba03ac00691c3e02ff67a685285480785d86e98f491368e053ddf155b29c2d0 (100MB, v14.11.0.49, versionCode 295722)
- smali/com/snap/backup/api/MushroomBackupAgent.smali – SC-01 backup agent registration
- smali/GYf.smali – SC-01 fideliusKeys schema, SC-02 internal URLs, SC-07 canUseMySelfie
- smali/com/snap/shake2report/controller/screenshot/CaptureScreenService.smali – SC-04
- smali/ETh.smali – SC-06 snapads_dsa_illegal_content_report
- smali/u6c.smali – SC-03 LIVE_LOCATION, NEAR_ME_GHOST_MODE
- res/values/strings.xml – SC-05 Facebook and Google credentials
- AndroidManifest.xml – full permission list, allowBackup, MushroomBackupAgent declaration

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent to security@snap.com, 7 findings, bcc DSB/EDPB/ICO (bounced)/ CERT.at/Coimisiun na Mean
2026-06-27	7-day follow-up; automated ticket acknowledgment received same day, ticket N2LX1Z
2026-06-29	Full evidence submission filed with Coimisiun na Mean, CAS-09535
2026-07-16	Coimisiun na Mean states only Irish-located complainants can file directly; RFI-IRFOS contests the framing twice the same day
2026-07-23	27-day follow-up to Snap, no reply
2026-08-12	RTR (Austria's DSC) formally transmits the case to Coimisiun na Mean under DSA Art. 53/57 cooperation
2026-08-14 / 08-24 / 08-31	48-, 58-, and 65-day follow-ups to Snap, no reply
2026-09-04	70-day follow-up reformulates SC-01 as an explicit yes/no question: does Snap retain server-side Fidelius decryption capability

Date	Event
2026-09-16, 16:59 UTC	Snap opens a new, unrelated ticket (#274553938); ”Shawn” replies with generic boilerplate, no findings addressed
2026-09-16, 17:09 UTC	RFI-IRFOS notes the new ticket does not answer the open question, restates SC-01 in full
2026-09-16, 21:47 UTC	Snap’s DSA Team gives its first and only specific technical response: disputes that the backed-up SharedPreference archives include the cited database field or message payloads; states its review of SC-01 is complete
2026-09-17, 00:35 UTC	RFI-IRFOS declines to provide further uncompensated material, confirms its own review is complete, embargo unchanged
2026-09-19	Embargo closes; this report publishes

Snap’s 16 September response is the only substantive, finding-specific reply RFI-IRFOS received across seven findings and 91 days, and it deserves to be read as exactly that: a real technical rebuttal, not a deflection template. It settles one narrow question, whether two specific SharedPreference archive names correspond to a specific SQLite column, in Snap’s favor as far as this analysis can independently confirm, since neither party captured a live backup archive. It does not settle the broader server-side decryption capability question, which remains open in writing, and it does not touch SC-02 through SC-07, which close this embargo period exactly as reported, unaddressed.

Positive Observations

- No Android Privacy Sandbox usage (no FLEDGE Custom Audience API, no Topics API) – no on-device behavioral ad profiling, a meaningful contrast to several peer platforms audited under this programme.
- DETECT_SCREEN_CAPTURE and DETECT_SCREEN_RECORDING are implemented, actively monitoring third-party recording of Snapchat content.
- Fidelius end-to-end encryption is enabled by default for all new friends (isFideliusReady = 1).
- Ghost Mode gives users a working, genuine opt-out from real-time SnapMap location sharing.
- AI chatbots are explicitly flagged and distinguished from human contacts in the data model (isAiChatbot = 0 by default).
- canUseMySelfie defaults to disabled, correct design for a biometric-processing feature, independent of the open question over its consent-capture flow (SC-07).

Residual Risk & Recommendations

- SC-01: publish a reproducible backup-capture test settling the SharedPreference-content dispute, and answer in writing whether any server-side Fidelius decryption capability exists, for any content class.
- SC-03: scope ACCESS_BACKGROUND_LOCATION to active, user-initiated SnapMap sessions only, with auto-revocation, and verify a separate, informed consent step for minors independent of install-time permission grants.
- SC-04: apply FLAG_SECURE across all ephemeral-content viewer activities so accidental capture is not possible regardless of the trigger gesture.
- SC-05: rotate the exposed Facebook client token and confirm server-side certificate-fingerprint restriction on the Google API key.
- SC-06: build a DSA Art. 16 compliant in-app illegal-content reporting path covering every content surface, not only advertisements, ahead of the next Art. 33 systemic-risk assessment cycle.
- SC-07: publish the actual consent-capture flow for canUseMySelfie against the GDPR Art. 9(2)(a) explicit-consent standard, and confirm Dreams output carries an AI-generated disclosure per the EU AI Act.
- SC-02: apply ProGuard/R8 comment stripping to all future release builds; this class of internal-infrastructure leak is fully preventable at build time.

RFI-IRFOS rfi.irfos@gmail.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria Coordinated disclosure per ISO/IEC 29147. Research activity protected under Austria's Forschungsfreiheitsgesetz (Art. 17 StGG). GDPR Art. 5, 6, 8, 9, 13, 32. DSA Art. 16, 27, 33, 53, 57. REF SNAPCHAT-2026-R1.