Coordinated Security & Privacy Disclosure, Final Report

Meta Platforms: WhatsApp, Facebook, Instagram, Messenger

Systemic cross-platform audit, four Android apps, approximately 3.3 billion daily active users

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – NINETY-ONE DAYS, EIGHT WRITTEN NOTICES, ZERO REPLIES OF ANY KIND

Target	Meta Platforms, Inc., Menlo Park, California, US / Meta Platforms Ireland Limited, Dublin (EU controller)
Products audited	WhatsApp (com.whatsapp) 2.26.23.74, Facebook (com.facebook.katana) 566.0.0.48.73, Instagram (com.instagram.android) 433.0.0.47.68, Messenger (com.facebook.orca) 566.0.0.57.86
Disclosure reference	REF META-2026-R1 / META-FOLLOWUP-2026-09
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (S3 shadow profiles, CVSS v4.0 8.7 High) / S4 zero cert pinning scores 8.6 High

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 20 June 2026, RFI-IRFOS performed static analysis of the production Android APKs for WhatsApp, Facebook, Instagram, and Messenger. The nine findings below, five CRITICAL and four HIGH, are addressed collectively because they describe a single cross-platform data architecture, not isolated defects in four separate apps: a shared device identifier links activity across all four, a shadow-profile system uploads the hashed phone numbers of people who have never used any Meta product, encryption key material for Messenger's marketed end-to-end encryption is retrievable from Meta's own servers, and all four platforms ship with zero Android certificate pinning.

Meta's Irish Data Protection Commission, its lead GDPR supervisory authority, fined Meta approximately 2.3 billion euros across five decisions between March 2022 and May 2023, covering forced consent for advertising, unlawful US data transfers, large-scale data scraping, and Instagram's handling of children's data. The findings in this report are structurally distinct from all five: they concern encryption-key custody, a non-user shadow-profiling database schema, an undisclosed AI data flow inside end-to-end encrypted chats, absent transport security, and on-device automated ad-targeting decisions, none of which were the subject of those prior fines.

RFI-IRFOS sent eight written notices to privacy@meta.com and security@meta.com over 91 days. None produced a reply of any kind, not an automated ticket, not a bounce, not a human acknowledgment. This is the only target in RFI-IRFOS's entire June 2026 disclosure wave, encompassing well over a hundred applications, for which that is true. The findings below stand exactly as sent, unanswered and unaddressed.

Scope: Static analysis of the publicly downloaded production Android APKs only, cross-referenced against Meta's own published privacy disclosures and Apple App Store Privacy Nutrition Labels. No Meta backend, account, or infrastructure was accessed or tested.

Disposition

R1 sent 20 June 2026 to privacy@meta.com and security@meta.com, bcc Austrian DSB, CERT.at, the Irish Data Protection Commission as Meta's lead GDPR supervisory authority, and the EDPB. Eight written notices followed over 91 days: 27 June, 28 June, 17 July, 27 July, 9 August, 24 August, 4 September, and 16 September 2026. Not one produced a reply of any kind, not a ticket number, not an automated acknowledgment, not a bounce, not a human. Every other target audited in the same June 2026 wave produced at least an automated acknowledgment. Meta did not.

ID	Severity	Title
S1	CRITICAL	Messenger: server-side encryption key retrieval invalidates end-to-end encryption claims
S2	CRITICAL	WhatsApp: Meta AI context menu inside private end-to-end encrypted chats

ID	Severity	Title
S3	CRITICAL	Facebook: shadow profile architecture confirmed in production database schema
S4	CRITICAL	Zero certificate pinning across all four platforms
S5	CRITICAL	Facebook: ACCESS_ADSERVICES_CUSTOM_AUDIENCE, on-device behavioral ad-auction profiling
H1	HIGH	All four platforms detect screen recording and screenshots, an anti-transparency measure
H2	HIGH	Instagram: READ_CALL_LOG embedded via Ray-Ban Meta AI glasses integration
H3	HIGH	WhatsApp, Facebook, and Instagram jointly declare READ_CALL_LOG
H4	HIGH	FAMILY_DEVICE_ID: technical proof of cross-app identity linkage

Subject & Operator Analysis

Meta Platforms, Inc. (Menlo Park, California) is the global operator; Meta Platforms Ireland Limited (Dublin) is the entity of record for EU/EEA GDPR purposes, making Ireland's Data Protection Commission the lead supervisory authority. Facebook and Instagram are EU-designated Very Large Online Platforms under the Digital Services Act, placing them under additional Art. 27 algorithmic-transparency and Art. 33 systemic-risk-assessment obligations beyond the GDPR analysis in this report. The four audited applications collectively report approximately 3.3 billion daily active users.

Architecture & Data Flow

- FAMILY_DEVICE_ID: a shared cross-application identifier linking WhatsApp, Facebook, Instagram, and Messenger activity on the same device (H4).
- Shadow-profile pipeline: device contacts hashed locally (contacts_upload_snapshot, phone_address_book_snapshot) and uploaded via xfb_xccu_contact_upload, independent of whether the contact has ever used a Meta product (S3).
- Messenger key-custody path: get_server_encryption_key and related strings describe encryption key material retrievable from Meta's servers, including for logged-out users (S1).
- WhatsApp-to-Meta-graph bridge: hardcoded b-graph.facebook.com and i.instagram.com GraphQL endpoints in the WhatsApp binary, plus the in-chat Meta AI entry point that exits the end-to-end encryption boundary on invocation (S2).
- Zero network_security_config.xml across all four binaries, meaning no certificate pinning anywhere in the architecture (S4).
- Facebook's Android Ad Services declarations, including ACCESS_ADSERVICES_CUSTOM_AUDIENCE, the only occurrence of this permission across RFI-IRFOS's full audit series (S5).

Findings

S1: Messenger: server-side encryption key retrieval invalidates end-to-end encryption claims

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

Production Messenger APK strings: get_server_encryption_key, GetServerEncryptionKeyLoggedOutResponsePayload, Received 0 usable keys from server, MSGEncryptedBackupsNetworkVerificationKeyPersistencePluginjni.

```
GetServerEncryptionKeyResponsePayload
get_server_encryption_key
GetServerEncryptionKeyLoggedOutResponsePayload
get_server_encryption_key_logged_out
Received 0 usable keys from server
MSGEncryptedBackupsNetworkVerificationKeyPersistencePluginjni
enforceOptionalServerKey=
```

Genuine end-to-end encryption means the server never possesses the encryption keys. get_server_encryption_key names the client fetching key material from Meta's server; GetServerEncryptionKeyLoggedOutResponsePayload means this occurs even for logged-out users; Received 0 usable keys from server is an error state confirming that normal operation involves key distribution from Meta's infrastructure. The Signal Protocol, which Meta states Messenger uses, is designed so key material is generated on-device and never transmitted to the service operator. No response was received naming this finding.

Impact: Meta retains the technical capability to decrypt Messenger conversations server-side, contrary to its own end-to-end encryption marketing and GDPR Art. 13(1)(e) security disclosure obligations.

Fix: Publish an independent, reproducible architecture review demonstrating that no key material capable of decrypting user content ever transits or is retrievable from Meta's servers, or disclose the actual key-custody model to users.

S2: WhatsApp: Meta AI context menu inside private end-to-end encrypted chats

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

ASK_META_AI_CONTEXT_MENU_1ON1 and ASK_META_AI_CONTEXT_MENU_GROUP place a Meta AI entry point inside private WhatsApp chats. Invoking it forwards conversation context to Meta's AI inference infrastructure, outside the E2E boundary.

```
ASK_META_AI_CONTEXT_MENU_1ON1
ASK_META_AI_CONTEXT_MENU_GROUP
ASK_META_AI_MEDIA_VIEWER_1ON1
FB_META_AI_EVAL_GEN_JUDGE_RESPONSE
AIVOICE_FAVICON_CALL_HISTORY

https://b-graph.facebook.com/graphql
https://i.instagram.com/graphql_www
```

No response was received naming this finding. The CVSS score reflects that the data flow requires the user to actively invoke Meta AI (UI:A), which lowers the Base score relative to the qualitative CRITICAL label; the report keeps that label because the transport-layer encryption users are shown says nothing about this application-layer exit path, and WhatsApp-only users who have never created a Facebook or Instagram account are still routed through Meta's cross-platform graph infrastructure (b-graph.facebook.com, i.instagram.com) regardless.

Impact: A user who trusts WhatsApp's end-to-end encryption promise and invokes Meta AI inside a private chat has that conversation's context transmitted to Meta's servers with no disclosure separate from the general privacy policy.

Fix: Disclose, at the point of invocation inside the chat itself, that Meta AI use forwards conversation context outside the end-to-end encryption boundary, and obtain separate, specific consent for that data flow under GDPR Art. 5(1)(b).

S3: Facebook: shadow profile architecture confirmed in production database schema

CRITICAL, 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

contacts_upload_snapshot and phone_address_book_snapshot tables hash and store every phone contact locally; xfb_xccu_contact_upload uploads them to Meta's servers, including contacts who have never created a Facebook account.

```
CREATE TABLE contacts_upload_snapshot (local_contact_id INTEGER PRIMARY KEY,
    contact_hash TEXT, contact_extra_fields_hash TEXT)
CREATE TABLE phone_address_book_snapshot (local_contact_id INTEGER PRIMARY KEY,
    contact_hash TEXT)
contacts_upload/last_upload_client_root_hash
xfb_xccu_contact_upload
XFBXCCUContactPointUploadResult
normalized_phone_number
```

No response was received naming this finding. This is the highest CVSS v4.0 score of the nine findings, 8.7, because the people whose data is processed here, non-users, have no relationship with Meta, no awareness of the processing, and no attacker precondition applies: the app simply reads the device address book, hashes every contact, and uploads the hashes. Under GDPR Art. 6, there is no legal basis for processing the personal data of a third party who never consented, is not a party to any agreement with Meta, and cannot exercise Art. 15-22 rights because they are unaware the processing occurs.

Impact: Every phone number in a Facebook user's contact list, including people who have never created a Facebook account, is hashed and uploaded to Meta's servers without their knowledge or consent, feeding profile-building and 'People You May Know' suggestions.

Fix: Obtain the affected non-user's own consent before processing their contact data, or delete non-user hashes and cease the upload entirely absent a valid Art. 6 legal basis.

S4: Zero certificate pinning across all four platforms

HIGH, CVSS v4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 8.6

0 network_security_config.xml files found across WhatsApp, Facebook, Instagram, and Messenger. No CertificatePinner or custom X509TrustManager in any of the four binaries.

No response was received naming this finding. Four platforms processing private messages, precise location, biometric face data, financial transactions, and inferred political and religious signals, reaching roughly 3.3 billion daily users collectively, trust the full system CA store with no pinning on any of the four apps simultaneously. This is not a minor oversight: certificate pinning is a standard, well-documented Android security measure, and its coordinated absence across all four platforms suggests a deliberate architectural choice, most plausibly to keep traffic-inspection tooling (debugging, A/B testing, ad measurement) from triggering pinning failures, rather than an isolated omission in one app.

Impact: An attacker in a position to intercept traffic on a compromised network, an MDM-injected corporate root, a compromised intermediate CA, or a state-level CA, can intercept or manipulate traffic to any of the four apps with no client-side detection.

Fix: Implement certificate pinning via network_security_config.xml with primary and backup pins, rotated on a schedule, across all four applications.

S5: Facebook: ACCESS_ADSERVICES_CUSTOM_AUDIENCE, on-device behavioral ad-auction profiling

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

Facebook declares all four Android Ad Services permissions simultaneously, including ACCESS_ADSERVICES_CUSTOM_AUDIENCE, the Android Protected Audience API for on-device behavioral ad-auction processing.

```
android.permission.ACCESS_ADSERVICES_AD_ID
android.permission.ACCESS_ADSERVICES_ATTRIBUTION
android.permission.ACCESS_ADSERVICES_TOPICS
android.permission.ACCESS_ADSERVICES_CUSTOM_AUDIENCE
```

No response was received naming this finding. Facebook is the only app in RFI-IRFOS's entire audit series to declare this specific permission. Behavioral interest-group matching against advertiser audiences, computed on-device, is automated decision-making under GDPR Art. 22 and requires specific disclosure under Art. 13(2)(f); RFI-IRFOS found no such specific disclosure in Meta's privacy notice.

Impact: Users are subject to on-device automated behavioral ad-targeting decisions that Meta's privacy notice does not specifically disclose as automated processing.

Fix: Disclose the use of the Android Protected Audience API as a specific instance of automated processing under GDPR Art. 13(2)(f), and provide the Art. 22 safeguards that automated decision-making requires.

H1: All four platforms detect screen recording and screenshots, an anti-transparency measure

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

SCREENSHOT_DETECTED and debug_screenshot_detection (Facebook, Messenger); MEDIA_OVERLAY_SCREEN_RECORDING_FLOW_LEAK_V432 (Instagram, naming the capture a 'leak').

No response was received naming this finding. The CVSS score is low because this finding has no direct confidentiality, integrity, or availability victim impact in the classic sense; the report keeps the qualitative HIGH label because a dedicated debug test suite for the detection system itself, present in two of the four apps, indicates deliberate investment in suppressing users' own ability to document platform behavior for journalism, regulatory evidence, or personal record-keeping, with no GDPR Art. 6(1)(f) legitimate interest basis that survives that purpose.

Impact: Users, journalists, and regulators attempting to document platform behavior via screen recording are detected and, per Instagram's own internal naming, treated as a 'leak' to suppress.

Fix: Remove screen-recording and screenshot detection outside of narrowly scoped, disclosed use cases such as DRM-protected media playback.

H2: Instagram: READ_CALL_LOG embedded via Ray-Ban Meta AI glasses integration

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

assets/com/facebook/smartglasses_ai/, ai_agent_voice_calling_enabled, and WA__AIVOICE_FAVICON__CALL_HISTORY confirm the Ray-Ban Meta AI glasses call-history integration ships inside the Instagram APK for all users, not only glasses owners.

No response was received naming this finding. Call logs reveal who a person called, when, for how long, and how often, a precise map of real-world relationships. Under GDPR Art. 5(1)(c), a photo and video sharing platform's core function requires no call log access; bundling a hardware accessory's permission into the base app for roughly 2 billion Instagram users who do not own the glasses does not meet data minimisation.

Impact: Instagram's approximately 2 billion users, the overwhelming majority of whom do not own Ray-Ban Meta glasses, carry a call-log permission justified by a feature they cannot use.

Fix: Gate READ_CALL_LOG behind an explicit, glasses-paired device state, never granted to the base Instagram install.

H3: WhatsApp, Facebook, and Instagram jointly declare READ_CALL_LOG

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

READ_CALL_LOG is declared independently by three of the four audited apps, enabling Meta to construct a near-complete cross-platform social graph from call metadata alone.

No response was received naming this finding. Combined with S3's contact-hash upload, call metadata across three platforms maps relationships including with people who have never used any Meta product, independent of message content.

Impact: A social graph constructed from call metadata across three independently-declarin g platforms reaches non-users as well as users.

Fix: Consolidate call-log access to a single, purpose-scoped, minimally privileged component rather than three independent declarations.

H4: FAMILY_DEVICE_ID: technical proof of cross-app identity linkage

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

FAMILY_DEVICE_ID and FBCredentialsStore/getFBIdentity in the production WhatsApp APK confirm a shared cross-application device identifier linking WhatsApp, Facebook, Instagram, and Messenger activity on the same device.

No response was received naming this finding. Meta's 2014 WhatsApp acquisition came with a public commitment to operate it independently; the 2021 WhatsApp privacy policy update, itself challenged by multiple European DPAs, partially disclosed cross-app integration in policy language. FAMILY_DEVICE_ID in the 2026 production APK is the technical confirmation that the integration is architectural, not an optional or disclosed-then-limited feature.

Impact: A user's WhatsApp-only activity is linkable to their Facebook, Instagram, and Messenger activity on the same device via a shared identifier, independent of whether they ever linked the accounts themselves.

Fix: Publish the actual scope of FAMILY_DEVICE_ID-linked data sharing between the four platforms and provide a working opt-out independent of account linking settings.

Impact Analysis: The Metadata Problem

No single finding in this report is necessarily unlawful in isolation. The four platforms collectively collect precise location, WiFi and Bluetooth identifiers enabling physical proximity and co-presence mapping, call log metadata, contact address books including non-users, biometric face data, behavioral interaction signals, payment history, and inferred political, religious, and health-adjacent attributes. The legal question, one several data protection authorities have already begun to address, is whether combining these signals into a persistent, cross-platform, real-time behavioral profile is something any user can meaningfully consent to through a single terms-of-service acceptance screen. RFI-IRFOS submits that it is not: GDPR Art. 4(11)'s requirement for consent that is freely given, specific, informed, and unambiguous cannot be satisfied by one consent event covering dozens of data categories, cross-platform linkage, third-party shadow profiling, AI inference, and on-device behavioral auction processing simultaneously.

S3's shadow-profile finding carries a particular weight: the people affected are not Meta users at all. They have never opened a Meta app, never accepted a Meta terms of service, and have no practical way to learn that their phone number sits, hashed, on Meta's servers because someone else's phone had their number saved.

Data Protection, Article by Article

Finding	Provision	Concern
S1	GDPR Art. 5(1)(f), Art. 13(1)(e), Art. 32	Server-side retrievable encryption key material contradicts the end-to-end encryption representation
S2	GDPR Art. 5(1)(b), Art. 13	Purpose-incompatible AI inference inside a private messaging context, undisclosed at point of use
S3	GDPR Art. 6, Art. 4(11)	No legal basis for processing non-users' hashed contact data
S4	GDPR Art. 32(1)(a)	No certificate pinning on any of four platforms carrying the most sensitive data categories
S5	GDPR Art. 22, Art. 13(2)(f)	Undisclosed on-device automated ad-targeting decision-making
H1	GDPR Art. 5(1)(a)	Anti-transparency screen-recording detection with dedicated debug tooling

Finding	Provision	Concern
H2, H3	GDPR Art. 5(1)(c)	Call-log access exceeding the stated purpose of a messaging or media-sharing app
H4	GDPR Art. 5(1)(b), Art. 13	Cross-app identity linkage beyond what was disclosed at the 2014 acquisition and the 2021 policy update

Regulatory & Legal Landscape

Date	Amount	Basis
March 2022	17 million euro	Data breach notification failures
September 2022	405 million euro	Instagram children's data handling
November 2022	265 million euro	Facebook data scraping, 533 million records
January 2023	390 million euro	Forced consent for targeted advertising
May 2023	1.2 billion euro	Unlawful US data transfers, insufficient standard contractual clauses

These five decisions total approximately 2.3 billion euro from Ireland's Data Protection Commission, Meta's lead GDPR supervisory authority, since March 2022. Every finding in this report concerns a distinct practice from all five: encryption-key custody, a non-user shadow-profiling schema, an undisclosed in-chat AI data flow, absent transport security, and on-device automated ad-targeting, none of which were the subject of the prior fines. This disclosure was bcc'd to the Austrian DSB, CERT.at, the Irish DPC, and the EDPB at every stage of the correspondence.

Indicators of Compromise & Reproducible Evidence

- WhatsApp (com.whatsapp) 2.26.23.74, Facebook (com.facebook.katana) 566.0.0.48.73, Instagram (com.instagram.android) 433.0.0.47.68, Messenger (com.facebook.orca) 566.0.0.57.86
- Messenger: get_server_encryption_key, GetServerEncryptionKeyLoggedOutResponsePayload, MSGEncryptedBackupsNetworkVerificationKeyPersistencePluginjni
- WhatsApp: ASK_META_AI_CONTEXT_MENU_1ON1, ASK_META_AI_CONTEXT_MENU_GROUP, FAMILY_DEVICE_ID, FBCredentialsStore/getFBIdentity
- Facebook: contacts_upload_snapshot, phone_address_book_snapshot, xfb_xccu_contact_upload, ACCESS_ADSERVICES_CUSTOM_AUDIENCE
- Instagram: assets/com/facebook/smartglasses_ai/, ai_agent_voice_calling_enabled, MEDIA_OVERLAY_SCREEN_RECORDING_FLOW_LEAK_V432
- All four: 0 network_security_config.xml files, confirmed absence of certificate pinning

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent to privacy@meta.com and security@meta.com, 9 findings, bcc Austrian DSB/CERT.at/Irish DPC/EDPB
2026-06-27 / 06-28	First follow-ups, no reply of any kind
2026-07-17 / 07-27	Continued follow-ups, no reply
2026-08-09 / 08-24	Continued follow-ups, no reply
2026-09-04	70-day follow-up, no reply
2026-09-12	Follow-up restating all three open questions, no reply
2026-09-16	Final notice, day 88, eight messages, still no ticket, acknowledgment, bounce, or human reply of any kind
2026-09-19	Embargo closes; this report publishes

Meta is the only target in RFI-IRFOS's entire June 2026 disclosure wave, spanning well over a hundred applications, to produce zero response of any kind across eight written notices and 91 days, not even an automated ticketing acknowledgment. Every one of the nine findings above stands exactly as originally reported, unconfirmed, undisputed, and unaddressed.

Residual Risk & Recommendations

- S1: publish an independent, reproducible architecture review of Messenger's actual key-custody model.
- S2: disclose, at the point of invocation, that Meta AI use inside a WhatsApp chat forwards content outside the end-to-end encryption boundary, and obtain separate consent for it.
- S3: obtain consent from, or cease uploading, the hashed contact data of individuals who have never used any Meta product.
- S4: implement certificate pinning with primary and backup pins, on a rotation schedule, across all four applications.
- S5: disclose the Android Protected Audience API's use as automated decision-making under GDPR Art. 13(2)(f) and Art. 22.
- H1: remove screen-recording and screenshot detection outside narrowly scoped, disclosed DRM use cases.
- H2/H3: scope READ_CALL_LOG to an explicit glasses-paired device state rather than the base app install.
- H4: publish the actual scope of FAMILY_DEVICE_ID cross-app data sharing and provide a working, independent opt-out.

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. 4, 5, 6, 9, 13, 22, 32. DSA Art. 27, 33. REF META-2026-R1.