Coordinated Security & Privacy Disclosure, Final Report

Uber Trilogy: Rider, Eats, Driver (com.ubercab, com.ubercab.eats, com.ubercab.driver)

Uber B.V., Amsterdam, Netherlands (EU controller); Uber Technologies, Inc., San Francisco (NASDAQ: UBER)

SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, 90 DAYS AFTER DISCLOSURE, EIGHT MESSAGES, ZERO REPLY OF ANY KIND

Target	Three Android applications sharing one telemetry platform: Uber Rider, Uber Eats, and Uber Driver
Packages	com.ubercab (Rider), com.ubercab.eats (Eats), com.ubercab.driver (Driver)
Operator	Uber B.V., Burgerweeshuispad 301, 1076 HR Amsterdam, Netherlands (EU controller); Uber Technologies, Inc., San Francisco, California, USA (parent, NASDAQ: UBER)
Initial Disclosure	2026-06-27
Original Embargo	2026-09-19 (90 days from disclosure, as stated in the original notice)
Report Published	2026-09-25, six days after the embargo, an internal publishing gap, not a change in terms
Regulators in CC/BCC	Austrian DSB, German BfDI, CERT.at, EDPS
Total Outbound Messages	8, across two threads and 90 days, to security@uber.com and privacy@uber.com, cc press@uber.com
Inbound Replies	0. No reply, automated or human, was ever received.

rfi.irfos@gmail.com • rfi-irfos.com
ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

On 27 June 2026, RFI-IRFOS disclosed to Uber that its three Android applications, Rider, Eats, and Driver, are not three separate products but one monolithic telemetry platform with three frontend interfaces, evidenced structurally in the binaries themselves: Eats ships as an embedded Dynamic Feature Module inside Rider, and the Driver and Eats apps share the identical Firebase API key, placing consumer food-delivery behavior and worker employment data in a single backend project.

The most serious finding is a genuine, demonstrated security vulnerability, not merely a disclosure gap: all three apps export a broadcast receiver, ParametersOverrideRequestBroadcastReceiver, with no permission requirement and no caller-identity check anywhere in its onReceive() implementation. Any application installed on the same device can send a two-line Intent that silently disables Uber's speed-intervention safety monitoring, with no log entry visible to the driver. A second finding documents mandatory real-time video and audio streaming from driver-facing cameras to remote participants via LiveKit and Twilio Video, framed to drivers as a consent decision whose dialog artwork Uber can modify remotely without an app update, inside an employment relationship where declining risks a worker's income, a framing GDPR Art. 7 does not recognize as valid consent.

Eight messages were sent across two correspondence threads to security@uber.com and privacy@uber.com, cc'ing press@uber.com and bcc'ing the Austrian DSB, the German BfDI, CERT.at, and the EDPS, across 90 days. Not one reply, automated or human, was ever received on either thread. The 90-day embargo, set at first contact, elapsed on 19 September 2026. This report and the accompanying closure notice publish six days later, an internal gap on RFI-IRFOS's side, not a change to the terms already disclosed.

Scope: Root-level static analysis of the production Uber Rider, Uber Eats, and Uber Driver Android applications (com.ubercab, com.ubercab.eats, com.ubercab.driver), covering the AndroidManifest, resource strings, and decompiled dex/smali of all three binaries, as pulled via ADB and reviewed on 25 June 2026. No dynamic instrumentation, live traffic capture, exploitation of the zero-authentication broadcast receiver against a live account, or interaction with Uber's backend infrastructure was performed.

Disposition

Five findings were disclosed on 27 June 2026, re-scored under CVSS v4.0. Two findings are held at CRITICAL under explicit, stated blast-radius escalations. A zero-authentication broadcast receiver present in all three apps, allowing any co-located application to silently disable safety systems including speed-intervention monitoring, reaches HIGH/7.0 on CVSS alone and is escalated to CRITICAL because the affected systems protect third parties, passengers, not just the app's own user. Mandatory real-time video and audio streaming from driver-facing cameras, framed as a consent decision inside an employment relationship where refusal risks income, reaches HIGH/8.7 on CVSS alone and is escalated to CRITICAL because GDPR Art. 7 does not recognize consent obtained under that kind of economic coercion as freely given. A persistent, cross-reset hardware fingerprint bridging worker and consumer identity remains at HIGH, matching its computed CVSS band exactly. A shared Firebase backend routing consumer and worker data into one project, and an undisclosed multi-layer algorithmic management system, correct to MEDIUM. Eight messages were sent across 90 days. Not one reply of any kind was ever received.

ID	Severity	Title
C1	CRITICAL	Zero-Authentication Broadcast Receiver in All Three Apps Lets Any Co-Located App Silently Disable Safety Systems
C2	MEDIUM	Shared Firebase Project Routes Consumer Food-Delivery Data and Worker Employment Data Into One Backend
C3	HIGH	Advertising ID Plus a Hardware DRM Fingerprint Bridge a Worker's Consumer and Employment Identity, and Persist Across Factory Reset
C4	CRITICAL	Mandatory Real-Time Video and Audio Streaming From Driver Cameras, Framed as Consent Inside an Employment Relationship Where Refusal Risks Income
C5	MEDIUM	Multi-Layer Algorithmic Management System, No Documented Art. 22 Safeguards

Subject & Operator Analysis

Rider, Eats, and Driver are three Android applications operated by Uber Technologies, Inc. through its EU controller Uber B.V. Structural evidence in the binaries themselves, an embedded Dynamic Feature Module and a shared Firebase project, establishes that these are not three independent products but one telemetry platform with three frontend interfaces.

Several genuine positives are worth naming. allowBackup=false is correctly set across all three apps. No third-party ad-mediation SDK (AppLovin, MoPub, or similar) was found in any of the three binaries. A network security configuration is present in all three, providing a correct baseline for certificate handling. The Twilio voice integration used for in-app driver-rider calls is a justified, disclosed feature, distinct from the video-streaming finding documented in C4.

Findings

C1: Zero-Authentication Broadcast Receiver in All Three Apps Lets Any Co-Located App Silently Disable Safety Systems

HIGH, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N, 7.0. RFI-IRFOS blast-radius escalation: raised from HIGH/7.0 to CRITICAL because the systems this vulnerability can silently disable, including speed-intervention monitoring, protect third parties, passengers riding with the driver, not only the app's own user, a real-world stake CVSS's technical scope does not weight.

ParametersOverrideRequestBroadcastReceiver is declared android:exported="true" with no android:permission attribute in all three apps. Its onReceive() implementation, confirmed in smali, reads namespace/key/value extras directly from the Intent and calls ParametersOverride.c() to write the value, with no checkCallingPermission(), checkCallingOrSelfPermission(), enforceCallingPermission(), getCallingUid(), or getCallingPackage() call anywhere in the method. Overrideable parameters include isSpeedInterventionInformationWorkerEnabled and other safety-relevant A/B experiment flags. Any application installed on the same device can send a two-line Intent to disable Uber's speed-intervention monitoring, with no log entry visible to the driver. RFI-IRFOS blast-radius escalation: raised from HIGH/7.0 to CRITICAL because the systems this can silently disable protect third parties, passengers riding with the driver, not only the app's own user.

```
AndroidManifest.xml (all three apps)
com.uber.parameters.override_broadcast.ParametersOverrideRequestBroadcastReceiver
android:exported="true"  # no android:permission attribute

Exception/attack: any co-located app can send:
Intent i = new Intent("com.uber.parameters.cli");
i.putExtra("namespace", "safety");
i.putExtra("key", "isSpeedInterventionInformationWorkerEnabled");
i.putExtra("value", "false");
context.sendBroadcast(i);
# onReceive() contains zero caller-identity checks before processing
```

Impact: A malicious app co-located on a driver's device can silently disable speed-intervention safety monitoring with no authentication, no signature check, and no visible log entry, a real-world safety risk extending to passengers, not only the device owner.

Fix: Require a signature-level permission on ParametersOverrideRequestBroadcastReceiver in all three apps and add explicit caller-identity verification in onReceive(). No confirmation that this has occurred was ever received.

C2: Shared Firebase Project Routes Consumer Food-Delivery Data and Worker Employment Data Into One Backend

---

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

The identical Firebase API key (AIzaSyBuQudVRtw2QE59911SkA7pNGFa-Scf0Ms) is present verbatim in both com.ubercab.driver and com.ubercab.eats, structural evidence that consumer food-order behavior and driver employment data, trip acceptance rates, speed events, location history, are processed within the same Firebase project. Six total Firebase keys are extractable from the three production binaries.

```
Shared key (Driver + Eats): AIzaSyBuQudVRtw2QE59911SkA7pNGFa-Scf0Ms
Rider-only keys:  AIzaSyA5bzbbJg0TEAQWIYvQS_WNcwNXWrpr8o4
                  AIzaSyDTrhOpIqfYqP3x9DMdbm-_GL28KBuCOGY
Eats-only key:    AIzaSyDkLKlyoJu4vsj53Bzk5pprBl50HOVxOsE
                  AIzaSyDywiKUisqJS75bNFdW5fOzRvk6CS-o_WE
```

Impact: Consumer analytics and driver employment data are architecturally routed through the same backend project, a purpose-limitation gap between two categories of data GDPR treats under different legal frameworks (ordinary consumer processing versus Art. 88 worker data).

Fix: Separate Driver's Firebase project from Eats' and Rider's, and rotate all six exposed keys with App Check and key restrictions applied. No confirmation that this has occurred was ever received.

C3: Advertising ID Plus a Hardware DRM Fingerprint Bridge a Worker's Consumer and Employment Identity, and Persist Across Factory Reset

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. This finding reaches HIGH on the computed CVSS v4.0 score alone; no editorial escalation was applied or needed.

The Driver app's BlockingDeviceFingerprint class, confirmed in smali, accepts a GoogleAdvertisingId, an AppSetIdInfoEntity, and a MediaDrmId together. The advertising ID is used for MARKETING_ATTRIBUTION_V2, meaning a worker's consumer advertising profile, built from behavior in Rider and Eats, is linked to their employment behavior in Driver via the shared identifier. MediaDrmId is a hardware-level identifier tied to the device's DRM subsystem that persists across application reinstallation and, where DRM state is preserved, factory reset, undisclosed in any driver privacy policy reviewed.

```
com.ubercab.driver smali
BlockingDeviceFingerprint constructor:
  accept(GoogleAdvertisingId, AppSetIdInfoEntity, MediaDrmId)
AndroidManifest.xml: ACCESS_ADSERVICES_ATTRIBUTION, ACCESS_ADSERVICES_AD_ID,
  com.google.android.gms.permission.AD_ID
```

Impact: A worker's advertising profile, built from their own consumer behavior across Uber's apps, is linked to their employment activity via a device fingerprint that persists even across a factory reset, a form of identity that cannot practically be reset by the person it identifies.

Fix: Remove MediaDrmId from BlockingDeviceFingerprint, or document an explicit, disclosed Art. 88 legal basis for combining a worker's advertising and employment identity. No confirmation that this has occurred was ever received.

C4: Mandatory Real-Time Video and Audio Streaming From Driver Cameras, Framed as Consent Inside an Employment Relationship Where Refusal Risks Income

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. RFI-IRFOS blast-radius escalation: raised from HIGH/8.7 to CRITICAL because GDPR Art. 7 does not recognize consent obtained under the economic coercion of an employment relationship as freely given, and the finding here is that mandatory streaming is framed to drivers precisely as a consent decision.

The Driver app ships a complete real-time audio/video streaming stack, LiveKit, Twilio Video, and a direct Camera2 recorder, operating under the internal name SIAR (Safety Incident Audio/video Recording). The confirmed string RemoteVideoTrackPublished establishes that video is streamed to remote participants, not merely recorded locally. The consent dialog's artwork is loaded from Uber's own servers at runtime, meaning Uber can alter the consent framing remotely without an app update. RFI-IRFOS blast-radius escalation: raised from HIGH/8.7 to CRITICAL because GDPR Art. 7 does not recognize consent obtained under the economic coercion of an employment relationship as freely given, and the finding here is that mandatory streaming is framed to drivers precisely as a consent decision, with no alternative legal basis stated.

```
com.ubercab.driver, confirmed strings
mandatory_record_applicability_based_device_features_enabled
siar_mandatory_recording_consent_dialog_artwork_url
VideoSessionEvent$RemoteVideoTrackPublished
VideoSessionEvent$RemoteAudioTrackPublished
FOREGROUND_SERVICE_CAMERA (manifest permission)
```

Impact: Drivers who decline real-time audio/video streaming inside a consent dialog whose framing Uber can alter remotely risk their ability to continue working, the opposite of freely given consent, while no disclosed Art. 6(1)(b) or (c) legal basis is stated as the actual ground for this processing.

Fix: State the actual legal basis for SIAR explicitly, most plausibly Art. 6(1)(b) or (c), not a consent dialog that cannot be freely declined in an employment context, and provide the Art. 13 transparency this scope requires. No confirmation that this has occurred was ever received.

C5: Multi-Layer Algorithmic Management System, No Documented Art. 22 Safeguards

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

The Driver app runs on-device ML activity recognition (ActivityRecognitionPluginWorker, BehaviorProcessorResults), speed-intervention monitoring with audio alerts, destination-lingering time tracking, and continuous data streaming to Uber's internal Carbon platform, with REQUEST_IGNORE_BATTERY_OPTIMIZATIONS ensuring these systems keep running in the background. Workers are confirmed subjects of undisclosed A/B experiments via getMlActivityRecognitionShadowModeMainXp(). No documentation with the Art. 22 specificity this scope requires, explanation of automated-decision logic, a right to human review, a right to contest, was located for this processing.

Impact: Workers are subject to continuous, multi-layer behavioral monitoring and algorithmic management running even when the app is not actively in use, with no documented right to explanation, human review, or contest as GDPR Art. 22 requires for automated decisions affecting them.

Fix: Publish Art. 22-compliant documentation of the automated-decision logic affecting drivers, including a right to human review and to contest, and disclose the A/B experimentation program explicitly. No confirmation that this has occurred was ever received.

Impact Analysis

C1 and C4 are the two findings escalated to CRITICAL, and they are escalated for different reasons: C1 because the zero-authentication vulnerability threatens the physical safety of third parties, passengers, not only the app's own user, and C4 because it names a specific, structural failure of consent validity inside an employment relationship, precisely the category of coercion GDPR Art. 7 exists to prevent. C2, C3, and C5 together describe an architecture where a driver's consumer identity, employment behavior, and biometric-adjacent monitoring data converge in ways none of the individual apps' own privacy disclosures account for.

Eight Messages, 90 Days, Zero Reply

This case's correspondence record is total silence. Eight messages were sent across two threads to security@uber.com and privacy@uber.com, cc'ing press@uber.com, and bcc'ing the Austrian DSB, the German BfDI, CERT.at, and the EDPS, across 90 days. Not one reply, automated or human, was ever received on either thread.

Data Protection, Article by Article

The findings map onto a small, specific set of GDPR and national employment-data provisions, set out below in one place instead of scattered across the findings themselves.

Article	Finding	Basis
Art. 32, Art. 5(1)(f)	C1	Zero-authentication broadcast receiver, safety-system manipulation available to any co-located app.
Art. 5(1)(b), Art. 88	C2	Shared backend architecture between consumer and worker data categories.
Art. 5(1)(b), Art. 22, Art. 88	C3	Persistent hardware fingerprint bridging consumer advertising and employment identity.
Art. 7, Art. 13, Art. 88	C4	Coercive consent framing for mandatory real-time worker surveillance.
Art. 22, Art. 13, Art. 88	C5	Undocumented automated-decision system affecting workers, no Art. 22 safeguards shown.

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 CVSS v4.0 is RFI-IRFOS's scoring guideline, not a ceiling or a floor. It gives a reproducible, third-party-legible starting point for severity, and it does not capture real-world blast radius on its own, factors such as user population size, a vulnerable or protected class of users, or a standing corporate governance exposure the technical vector alone cannot express. RFI-IRFOS reserves the right to weigh that blast radius above the bare CVSS score, and, more rarely, to hold a score below what CVSS alone would suggest when the underlying claim is unconfirmed or disputed with evidence. In this report, C1 is escalated from HIGH/7.0 to CRITICAL because the affected safety systems protect third parties, and C4 is escalated from HIGH/8.7 to CRITICAL because of a structural consent-coercion failure in an employment context, both real-world

circumstances CVSS's technical vector does not capture; C3 reaches HIGH on its computed score alone; C2 and C5 correct to MEDIUM. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: UBER-TRILOGY-2026.