Coordinated Privacy Disclosure, Final Report

Trip.com Android (ctrip.english)

Trip.com Group Limited (NASDAQ: TCOM); Trip.com Europe B.V., Amsterdam

SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, 92 DAYS AFTER DISCLOSURE, TWELVE MESSAGES, SEVEN BOUNCED, ZERO REPLY OF ANY KIND

Target	Trip.com, a major international travel booking platform, package still labeled ctrip.english, never rebranded
Package	ctrip.english
Operator	Trip.com Group Limited (NASDAQ: TCOM), Cayman Islands holding, majority PRC-shareholder-controlled; Trip.com Europe B.V., Amsterdam, Netherlands (EU establishment)
Initial Disclosure	2026-06-25
Original Embargo	2026-09-23 (90 days from disclosure, as stated in the original notice)
Report Published	2026-09-25, two days after the embargo, an internal publishing gap, not a change in terms
Regulators in BCC	Dutch Autoriteit Persoonsgegevens (lead SA), Austrian DSB, CERT.at, EDPS
Total Outbound Messages	12, across 92 days, all to privacy@trip.com. Seven of the first eight bounced outright; the address began accepting mail from 18 August 2026 onward.
Inbound Replies	0. No reply, automated or human, was ever received once the address began accepting mail.

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

Contents

Executive Summary

On 25 June 2026, RFI-IRFOS disclosed to Trip.com Group Limited that its Android application, still carrying the package name ctrip.english from its pre-rebrand Ctrip identity, permits cleartext HTTP transmission across the entire binary while collecting passport numbers via live camera OCR for flight-booking auto-fill, meaning a traveler scanning their passport on an airport or hotel WiFi network, the app's primary use context, can have that data intercepted in transit.

The same binary routes data through five independently identified processors, Tencent, Ant Group/Alipay, Baidu, Huawei, and UnionPay, each individually subject to compelled-disclosure obligations under the PRC National Security Law Art. 7, while Trip.com Group itself is majority-controlled by PRC-resident institutional shareholders and operates its core engineering from Shanghai, making the controller subject to the same law as the processors it uses. No EU adequacy decision covers any of these five simultaneous international transfers.

Twelve messages were sent to privacy@trip.com across 92 days, cc'ing the EDPS on one round and bcc'ing the Dutch Autoriteit Persoonsgegevens, the Austrian DSB, and CERT.at throughout. Seven of the first eight attempts bounced outright, the address only began accepting mail from 18 August 2026 onward. Not one reply, automated or human, was ever received at any point, before or after the address started accepting delivery. The 90-day embargo, set at first contact, elapsed on 23 September 2026. This report and the accompanying closure notice publish two 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 Trip.com Android application (ctrip.english, version 8.51.2, 98.2 MB), covering the AndroidManifest, resource strings, and decompiled dex/smali, as pulled via ADB and reviewed on 25 June 2026. No dynamic instrumentation, live traffic capture, or interaction with Trip.com's backend infrastructure was performed.

Disposition

Nine findings were disclosed on 25 June 2026, re-scored under CVSS v4.0. One finding independently reaches CRITICAL on the computed CVSS score alone: five simultaneous data flows to processors independently subject to the PRC National Security Law's compelled-disclosure obligations (Tencent, Ant Group/Alipay, Baidu, Huawei, and UnionPay), alongside a controller majority-owned by PRC-resident shareholders, with no EU adequacy decision covering any of the transfers. Cleartext HTTP permitted in an application that collects passport numbers via live camera OCR, and undisclosed IMEI plus multi-OEM device fingerprinting via the Adjust SDK, both reach HIGH on their own computed scores. Six further findings correct to MEDIUM. Twelve messages were sent across 92 days; seven of the first eight bounced outright before the address began accepting mail, and not one reply of any kind, automated or human, was ever received once it did.

ID	Severity	Title
C1	HIGH	Cleartext HTTP Permitted in an Application That Scans Passport Numbers
C2	CRITICAL	Five Independent PRC-NSL-Obligated Processors, Plus a PRC-Controlled Controller, No EU Adequacy Decision
C3	MEDIUM	Firebase Initializes Before Any Consent Screen
H1	MEDIUM	eSIM Write and Device-Policy-Level Subscription-Management Permissions, No Documented Purpose
H2	HIGH	Adjust SDK Ships IMEI Collection Plus Multi-OEM Device Fingerprinting Modules
H3	MEDIUM	Screenshot Detection on Booking Confirmations and Passport Scans
H4	MEDIUM	AppsFlyer Attribution With Hardcoded Direct Tracking Links
H5	MEDIUM	Boot-Persistent Background Operation With Microphone-Capable Foreground Service
M1	MEDIUM	Three PRC-OEM Push Notification Channels

Subject & Operator Analysis

Trip.com is a major international travel booking platform operated by Trip.com Group Limited (NASDAQ: TCOM), a Cayman Islands holding company majority-controlled by PRC-resident institutional shareholders, with EU operations conducted through Trip.com Europe B.V. in Amsterdam. The Android package name, ctrip.english, still carries the app's pre-rebrand Ctrip identity.

Several genuine positives are worth naming. allowBackup is correctly set to false. A network security configuration is present, though overridden by the application-level cleartext permission documented in C1. Biometric authentication is correctly implemented via USE_BIOMETRIC. The presence of Adjust's dedicated GDPR endpoint suggests some awareness of EU compliance requirements, even where the IMEI-collection module documented in H2 undermines it.

Twelve Messages, Seven Bounces, Then Total Silence

This case's correspondence record has two distinct phases. Seven of the first eight messages, sent between 25 June and 12 August 2026, bounced outright from privacy@trip.com. The address began accepting mail from 18 August 2026 onward. From that point through the final message on 12 September 2026, four further messages were delivered successfully. Not one reply, automated or human, was ever received, neither during the bounce phase nor after delivery began succeeding.

Findings

C1: Cleartext HTTP Permitted in an Application That Scans Passport Numbers

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

android:usesCleartextTraffic="true" is set at the application level, permitting unencrypted HTTP for any connection not explicitly pinned in the network security configuration. The app collects passport numbers via live camera OCR and transmits them to Trip.com's own passport gateway API. The application's primary use context, airports and hotels, is precisely the environment with the most adversarial, open WiFi infrastructure available to an attacker.

```
AndroidManifest.xml: android:usesCleartextTraffic="true"

confirmed passport-handling strings:
"Image uploaded directly to passportOcr interface"
https://m.trip.com/restapi/passport/gateway/%s/%s
```

Impact: A traveler scanning their passport to auto-fill a flight booking, while connected to an airport or hotel WiFi network, has that passport number exposed to interception by anyone else positioned on the same network.

Fix: Set cleartextTrafficPermitted="false" application-wide and route all passport-gateway traffic through certificate-pinned HTTPS exclusively. No confirmation that this has occurred was ever received.

C2: Five Independent PRC-NSL-Obligated Processors, Plus a PRC-Controlled Controller, No EU Adequacy Decision

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:H/SI:N/SA:N, 9.2. This finding reaches CRITICAL on the computed CVSS v4.0 score alone; no editorial escalation was applied or needed.

The binary integrates five independently identified processors, each individually subject to compelled-disclosure obligations under China's National Security Law Art. 7: Tencent (WeChat mini-program and business webview integration), Ant Group/Alipay (payment and financial-security SDK), Baidu (location/geocoding SDK sending GPS coordinates to Baidu servers), Huawei (install-referrer and payment-callback services), and UnionPay (state-owned payment infrastructure). Trip.com Group Limited itself is majority-owned by PRC-resident institutional shareholders and operates its core engineering from Shanghai, meaning the controller is subject to the same compelled-disclosure law as the five processors it uses. No EU adequacy decision covers any of these five simultaneous international transfers.

```
Tencent: content://com.tencent.mm.sdk.comm.provider/launchWXMiniprogram
Ant/Alipay: com.alipay.android.app.flybird.ui.window.FlyBirdWindowActivity
Baidu: https://api.map.baidu.com/sdkproxy/v2/lbs_locsdk/geocoding/v3/
Huawei: com.huawei.hms.ads.installreferrer.api.InstallReferrerClient
UnionPay: com.unionpay.tsmservice
# Controller: Trip.com Group Ltd, majority PRC-resident shareholder control,
# core engineering based in Shanghai
```

Impact: EU traveler data, including passport numbers, itineraries, and payment information, flows through five separate processors and a controller, all independently subject to PRC compelled-disclosure obligations, with no adequacy decision covering any of the resulting transfers.

Fix: Document an Art. 44-49 transfer mechanism for each of the five processors individually, or remove non-essential PRC-NSL-obligated dependencies from the EU-distributed build. No confirmation that this has occurred was ever received.

C3: Firebase Initializes Before Any Consent Screen

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.

FirebaseInitProvider is declared with android:initOrder=99 (0x63), meaning it initializes before any Activity, and therefore before any consent screen, can render.

Impact: App-open telemetry begins before the user has seen a single privacy notice.

Fix: Defer FirebaseInitProvider's initialization until after an app-native consent flow has run. No confirmation that this has occurred was ever received.

H1: eSIM Write and Device-Policy-Level Subscription-Management Permissions, No Documented Purpose

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

WRITE_EMBEDDED_SUBSCRIPTIONS and MANAGE_DEVICE_POLICY_MANAGED_SUBSCRIPTIONS, among the highest-privilege telephony permissions available to a non-carrier Android app, are both declared. A travel booking app has no evident business purpose requiring eSIM profile write access or device-policy-level subscription management.

Impact: The app carries permission scope, eSIM profile writing and MDM-level subscription management, that exceeds what a travel booking application's disclosed functionality requires.

Fix: Remove both permissions unless a specific, documented feature (e.g. travel eSIM provisioning) requires them, and disclose that feature explicitly if so. No confirmation that this has occurred was ever received.

H2: Adjust SDK Ships IMEI Collection Plus Multi-OEM Device Fingerprinting Modules

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 Adjust attribution SDK's own GDPR endpoint (gdpr.adjust.com) is present, but so is its IMEI-collection module alongside separate device-fingerprinting modules for Xiaomi, Huawei, Vivo, Samsung, and Meta OEM ecosystems. IMEI is a permanent, non-resettable device identifier requiring explicit consent under EU law, and the multi-OEM fingerprinting modules are specifically built for cross-device profiling within Chinese OEM ecosystems.

```
com.adjust.sdk.imei.Util    -- IMEI collection module
com.adjust.sdk.oaid.Util    -- OAID (China advertising ID)
com.adjust.sdk.xiaomi.Util / huawei.Util / samsung.Util / vivo.Util / meta.Util
https://gdpr.adjust.com     -- GDPR endpoint present alongside the above
```

Impact: A permanent, non-resettable device identifier is collected via an attribution SDK that also carries dedicated cross-device fingerprinting modules for multiple OEM ecosystems, despite the same SDK's own GDPR-compliance endpoint being present in the binary.

Fix: Remove the IMEI-collection module and the OEM-specific fingerprinting modules, or gate their use behind explicit, granular consent distinct from ordinary attribution tracking. No confirmation that this has occurred was ever received.

H3: Screenshot Detection on Booking Confirmations and Passport Scans

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.

DETECT_SCREEN_CAPTURE allows the app to log when a user screenshots content within it, including booking confirmations, passport scans, or payment receipts. ACCESS_SURFACE_FLINGER, a system-level graphics compositor permission not normally available to standard apps, is also declared.

Impact: A user's decision to screenshot sensitive content, a passport scan or a payment receipt, is logged by the app, with no disclosed purpose for that specific signal.

Fix: Disclose the purpose of screenshot detection or remove it if it serves no documented product function, and clarify the presence of the system-level graphics permission. No confirmation that this has occurred was ever received.

H4: AppsFlyer Attribution With Hardcoded Direct Tracking Links

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 AppsFlyer attribution SDK is present with hardcoded, active Ctrip-branded tracking links confirming live use, connecting ad-click sources to actual flight bookings. AppsFlyer is a US company subject to the US CLOUD Act.

```
https://app.appsflyer.com/ctrip.english?mediasource=internal&campaign=flight
```

Impact: Booking behavior is linked to advertising attribution sources and routed to a US-based processor subject to CLOUD Act disclosure obligations, without individual disclosure of this specific data flow.

Fix: Name AppsFlyer individually as a data processor with a stated Art. 28 basis and transfer mechanism. No confirmation that this has occurred was ever received.

H5: Boot-Persistent Background Operation With Microphone-Capable Foreground Service

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 app registers for BOOT_COMPLETED, explicitly requests exemption from Android's battery-optimization system to remain running indefinitely in the background, and declares FOREGROUND_SERVICE_MICROPHONE, permitting a foreground service with microphone access to persist even while the app is backgrounded.

Impact: The app is architected to run continuously in the background from device boot, with a microphone-capable foreground service persisting even when not actively in use, beyond what a travel-booking app's core function requires.

Fix: Scope background persistence and microphone-capable foreground services to specific, disclosed features (e.g. active voice search), and remove the blanket battery-optimization exemption if not load-bearing. No confirmation that this has occurred was ever received.

M1: Three PRC-OEM Push Notification Channels

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.

Xiaomi MiPush, OPPO/ColorOS MCS, and OnePlus/Heytap MCS push channels are all declared, routing notification delivery through three separate PRC-connected infrastructure providers in addition to the five processors named in C2.

Impact: Notification delivery is routed through three additional PRC-connected infrastructure providers beyond the five already documented, each a separate data flow.

Fix: Consolidate push delivery to a single, disclosed channel with a documented transfer mechanism, or disclose all PRC-OEM push channels individually. No confirmation that this has occurred was ever received.

Data Protection, Article by Article

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

Article	Finding	Basis
Art. 32, Art. 5(1)(f)	C1	Cleartext transmission of passport-adjacent identity data in the app's primary, adversarial-network use context.
Art. 44-49, Art. 13(1)(e)	C2	Five simultaneous PRC-NSL-obligated processor relationships, plus a PRC-controlled controller, no adequacy decision.
Art. 7, Art. 25	C3	Consent-gated SDK bootstrap fires before any consent mechanism can apply.
Art. 5(1)(b), Art. 6(1)	H1	Excessive telephony/eSIM permission scope beyond documented purpose.
Art. 5(1)(a), Art. 6(1)	H2	Non-resettable device identifier collection plus multi-OEM cross-device fingerprinting.
Art. 5(1)(b)/(c)	H3	Undisclosed screenshot-detection logging on sensitive content.

Article	Finding	Basis
Art. 28, Art. 13(1)(e)	H4	Undisclosed US-based attribution processor, CLOUD Act exposure.
Art. 5(1)(c), Art. 7	H5	Boot-persistent background operation with microphone-capable foreground service.
Art. 13(1)(e), Art. 44-49	M1	Three additional undisclosed PRC-connected push-delivery channels.

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, C2 reaches CRITICAL on its computed CVSS v4.0 score alone, and C1 and H2 reach HIGH on their computed scores alone, no editorial escalation applied to any of the three; C3, H1, H3, H4, H5, and M1 correct to MEDIUM to match their own computed bands. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: #TRIPCOM-001.