Seventeen Children’s Apps, One Voice, Three Routes to China

Outfit7 Limited – Talking Tom & Friends portfolio

A COPPA-certified children’s ad network sits inside the same 17 apps as a Chinese ad network that knows exactly what audience it is reaching

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – EIGHTY-SEVEN DAYS, NINE MESSAGES, ZERO REPLIES OF ANY KIND

Analyst	RFI-IRFOS Research Team
Report date	2026-09-19
Portfolio	17 Android apps, Talking Tom & Friends franchise
Operator	Outfit7 Limited
Severity	CRITICAL
Findings	5 (3 CRITICAL, 2 HIGH)
R1 sent	2026-06-24
Embargo / coordinated disclosure	2026-09-19
Written notices sent	9
Substantive replies received, ever	0

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

Outfit7 Limited publishes at least 17 Android apps in the Talking Tom & Friends franchise, every one of them PEGI 3, marketed and used overwhelmingly by children. Root-level analysis of the portfolio, beginning with a full decompile of Talking Tom Cat and extended across the franchise, found something unusual not because any single finding is novel, but because of what sits next to what: KidoZ and SuperAwesome, two ad networks specifically built and COPPA-certified for children's apps, integrated in the same binaries as ByteDance's Pangle network and Mintegral (Mobvista), neither of which is permitted under COPPA for an audience under 13.

That coexistence is the finding underneath the findings. A company does not integrate a COPPA-certified children's ad network by accident. Outfit7 built the compliance-aware version of this portfolio and the non-compliant version into the same binary, at the same time, and shipped both. The non-compliant path routes a hardcoded, non-resettable device identifier and, in 15 of 17 apps, a permission that captures a child's voice, first through Outfit7's own China-based backend, then through ByteDance's advertising infrastructure, then through a second Chinese ad network – three independent, cumulative routes to China, none of them backed by a documented Art. 46 GDPR transfer mechanism.

This disclosure was sent on 24 June 2026. As of this report, 87 days and nine written notices later, Outfit7 has never once replied – not a denial, not an acknowledgment, not an automated ticket response. The addresses used are confirmed live and accepting mail. The silence is total, and it is the only finding in RFI-IRFOS's 2026 programme with that exact profile: full technical detail delivered, full regulatory exposure named, and not one word back.

Scope: Root-level static analysis (apktool decode, smali inspection, AndroidManifest.xml review, endpoint extraction) of Talking Tom Cat (com.outfit7.talkingtom, version 5.1.3.3751, ~92MB) as the primary decompiled subject, with the shared-SDK-signature pattern confirmed present across the remaining 16 titles in the portfolio via manifest and permission-level analysis. No backend was accessed, no live account created, no traffic intercepted. Every finding below is drawn from the publicly distributed binaries.

Disposition

Reported 24 June 2026 to dpo@outfit7.com, cc privacy@outfit7.com, with the Austrian DSB, German BfDI, UK ICO and French CNIL in BCC. Nine written notices sent over 87 days (24 June, 27 June, 2 July, 17 July, 12 August, 21 August, 28 August, 4 September, 11 September). Zero replies of any kind – substantive, denying, or automated – from any Outfit7 address across the entire period. Public disclosure proceeds 19 September 2026, unchanged since 24 June.

ID	Severity	Title
C1	CRITICAL	A COPPA-certified children's ad network and a China-based ad network that cannot legally serve children, in the same 17 apps

ID	Severity	Title
C2	CRITICAL	Hardcoded, non-resettable device identifier transmitted to a Chinese ad endpoint in 16 of 17 apps
C3	CRITICAL	A child's voice, captured, routed through Outfit7's own China backend, then two further Chinese ad networks
H1	HIGH	Mintegral (Mobvista, Guangzhou) integrated across the full portfolio, with a documented history of attribution-data scraping
H2	HIGH	Thirteen advertising SDKs portfolio-wide, eleven of them not child-safe by their own vendor classification, without a demonstrated consent mechanism

Subject & Operator Analysis

Outfit7 Limited is the publisher of record for the Talking Tom & Friends franchise, one of the most widely installed children's-entertainment app families globally. The company operates at a scale where a 17-app shared SDK stack is a deliberate infrastructure decision, not an accident replicated by chance across unrelated products – the same Pangle, Mintegral, and Outfit7-own-backend integration pattern recurs across every title analysed.

The named contacts on this disclosure, dpo@outfit7.com and privacy@outfit7.com, along with a named individual contact (xinyu.qian@outfit7.com), have received every one of the nine written notices in this thread. None has bounced. The addresses are live and accepting mail; the silence is not a delivery failure.

Architecture & Data Flow

Each of the 17 apps shares one architecture: a children's-mode presentation layer backed by KidoZ/SuperAwesome (the COPPA-certified path), running in parallel with a second, much larger advertising layer – Pangle, Mintegral, and nine further networks – that carries no audience-gating logic RFI-IRFOS could identify in the decompiled code. Both paths are active in the same build.

- Children's-safe ad layer: KidoZ, SuperAwesome (COPPA-certified, minority share of SDK footprint).
- China-bound ad layer: ByteDance/Pangle (3,704 smali classes in Talking Tom Cat), Mintegral (3,268 smali classes).
- Own-infrastructure layer: aas-gapi.talkingtomandfriends.cn, apps2.outfit7.cn – Outfit7's own China-hosted API endpoints, present in all 17 apps.
- Sensor layer: RECORD_AUDIO, active with 117 confirmed code call sites in Talking Tom Cat, declared in 15 of 17 apps portfolio-wide.
- Identifier layer: hardcoded IMEI transmission to Pangle's endpoint in 16 of 17 apps, a permanent non-resettable identifier.

Findings

C1: A COPPA-certified children's ad network and a China-based ad network that cannot legally serve children, in the same 17 apps

Knowledge of audience proven by the company's own SDK choices

ByteDance's Pangle SDK is integrated in all 17 apps analysed, alongside KidoZ and SuperAwesome – both explicitly COPPA-certified children's advertising networks. Smali class counts for Pangle range from 16 (a stub integration) to 3,838 per app depending on title; Talking Tom Cat's build carries the full 3,704-class integration.

The presence of KidoZ and SuperAwesome is not a coincidence or a legacy artifact. It demonstrates that Outfit7 built and maintains a compliance-aware advertising path for this exact portfolio. The Pangle and Mintegral integrations sit in the same builds, active, not behind any audience-gating logic that RFI-IRFOS could identify in the decompiled code.

Impact: Regulatory exposure is not speculative here: COPPA explicitly excludes ByteDance and Mintegral SDKs from serving children under 13, and Outfit7's own parallel use of certified alternatives is direct evidence the company understood this distinction and shipped the non-compliant path anyway.

Fix: Remove Pangle and Mintegral from every title in the portfolio, or gate them behind a verified-adult account tier separate from the children's-mode experience KidoZ/SuperAwesome already serve.

C2: Hardcoded, non-resettable device identifier transmitted to a Chinese ad endpoint in 16 of 17 apps

IMEI exfiltration, confirmed in code

The Pangle endpoint call is hardcoded with the device IMEI as a URL parameter, confirmed in Talking Tom Cat's decompiled traffic-construction code: a live example value (702f89a658bd1f189c6e8e24587cd9ce) sits directly in the union_imei parameter, with lang=zh present in the same request.

```
https://api16-access-sg.pangle.io/api/ad/union/sdk/get_ads/?aid=1371
https://api16-endcard-pack-sg.pangle.io/union/endcard/...?union_imei=702
    f89a658bd1f189c6e8e24587cd9ce&lang=zh
https://api16-access-ttp.tiktokpangle.us/service/2/app_log/
```

Impact: The IMEI is a permanent, non-resettable hardware identifier. Unlike an advertising ID, a user or a parent cannot reset it to break cross-app or cross-session tracking. Combined with the shared SDK stack across 17 titles in one franchise, this identifier is structurally capable of linking a child's activity across the entire portfolio.

Fix: Remove IMEI collection entirely from the ad-request payload; use a resettable, privacy-preserving identifier only, with documented consent.

C3: A child's voice, captured, routed through Outfit7's own China backend, then two further Chinese ad networks

Art. 9 GDPR biometric data, no adequacy decision anywhere in the chain

RECORD_AUDIO is declared and actively referenced (117 code call sites confirmed in Talking Tom Cat) in 15 of 17 apps. In parallel, all 17 apps ship Outfit7's own China-hosted API endpoints.

```
https://aas-gapi.talkingtomandfriends.cn
https://apps2.outfit7.cn
```

The reconstructed chain: a child's voice, captured via RECORD_AUDIO, first reaches Outfit7's own .cn-hosted backend, then ByteDance/Pangle's advertising infrastructure, then Mintegral. Three independent, cumulative transfer points into China, none backed by a documented Art. 46 GDPR safeguard anywhere RFI-IRFOS could identify.

Impact: A child's voice recording is special-category biometric data under Art. 9 GDPR. Routing it through three separate China-bound infrastructure paths, in a portfolio that simultaneously integrates certified children's-safe alternatives, is the single most serious finding in this report.

Fix: Immediately audit and document what RECORD_AUDIO is actually used for in each title; remove or fully re-architect any path by which captured audio, or metadata derived from it, could reach the .cn backend or either Chinese ad network.

H1: Mintegral (Mobvista, Guangzhou) integrated across the full portfolio, with a documented history of attribution-data scraping

Second independent Chinese ad-tech vendor

Mintegral is integrated in all 17 apps, 3,268 smali classes confirmed in Talking Tom Cat, 3,394 to 4,243 across the wider portfolio for the 6 titles where exact counts were extracted from the original R1 correspondence. Mintegral/Mobvista has a documented history of attribution-data scraping (DCN report, 2020).

Impact: A second, independent China-based data collector operating in parallel with Pangle, not a redundant integration – each represents its own transfer chain and its own exposure.

Fix: Same as C1/C3: remove or gate behind verified-adult access.

H2: Thirteen advertising SDKs portfolio-wide, eleven of them not child-safe by their own vendor classification, without a demonstrated consent mechanism

The full ad-network cocktail, one app's confirmed count

Talking Tom Cat alone integrates 13 distinct advertising SDKs. Eleven are not child-safe networks by their own stated positioning; only KidoZ and SuperAwesome are COPPA-certified for children's use.

SDK	Smali classes	Origin	Child-safe?
Meta/Facebook Audience Network	3,440	USA	No
ByteDance/Pangle	3,704	China	No
Mintegral	3,268	China	No
IronSource	3,237	Israel	No
BidMachine	1,792	–	No
Smaato	1,615	USA	No
Chartboost	1,478	USA	No
Unity Ads	1,462	USA	No
AppLovin	1,427	USA	No
InMobi	1,227	India	No
Vungle	746	USA	No
SuperAwesome	195	UK	Yes (COPPA)
KidoZ	~50	–	Yes (COPPA)
AdMob	123	USA	Conditional

Impact: Eleven networks with no child-safety certification, active in a PEGI 3 title, alongside two that are certified – the ratio itself shows the certified networks are not the primary monetisation path.

Fix: Portfolio-wide SDK audit; retain only COPPA-certified networks for the children's-mode experience; document Art. 7 consent flow for any network retained.

Impact Analysis

The affected population is, structurally, children under 13 – the exact audience KidoZ and SuperAwesome exist to serve safely, and the exact audience COPPA exists to protect from the eleven other networks integrated in the same builds. A child using any of these 17 apps has their voice, if RECORD_AUDIO is triggered, and a permanent device identifier, routed toward infrastructure with no demonstrated audience-appropriate handling.

This is not a hypothetical population. The Talking Tom & Friends franchise is one of the most-installed children's app families in the world; a finding replicated across 17 titles in that franchise is a finding at a scale few single-app audits in this programme have matched.

The Complete Chain: Install to Exposure

A parent installs a Talking Tom app for their child because it is rated PEGI 3 and because, if they check, they will find KidoZ and SuperAwesome named as the advertising partners – both legitimately COPPA-certified, both a genuinely reasonable basis for trust. What the store listing does not surface is that the same binary also carries Pangle, Mintegral, and nine further ad networks with no comparable child-safety certification, active in parallel.

The child plays. If the app's voice-interaction features trigger RECORD_AUDIO, that audio – biometric data under Art. 9 GDPR – is captured. The device's IMEI, a permanent identifier the family cannot reset, is transmitted to Pangle's endpoint alongside a language parameter set to Chinese. Both signals move first through Outfit7's own China-hosted backend infrastructure, then into ByteDance's advertising pipeline, then into Mintegral's. None of these three hops is documented against an Art. 46 GDPR transfer safeguard anywhere RFI-IRFOS could locate in the binary or in Outfit7's public disclosures.

Causality, compressed

A compliance-aware SDK choice (KidoZ/SuperAwesome) proves audience knowledge. Audience knowledge, combined with the parallel non-compliant SDK choice (Pangle/Mintegral), causes a live, active exposure path for a child's voice and a permanent device identifier into China, three hops deep. That exposure, disclosed in full technical detail on 24 June, causes nine written notices over 87 days. Nine notices with zero replies of any kind causes publication on 19 September – the same mechanism this programme applies without exception, reached here after more silence than any other case in the 2026 corpus.

Child Protection & Developmental Harm

This is the section every other finding in this report exists to support. A child cannot consent under GDPR Art. 8; a parent's consent, where it exists at all in Outfit7's flow, cannot reasonably be understood to cover routing a voice recording through three sequential China-bound infrastructure hops when the same app simultaneously advertises COPPA-certified partners as its child-safety posture. The RECORD_AUDIO finding (C3) is the single highest-stakes item in this report precisely because voice is not a behavioural signal that can be anonymised after the fact – it is the child's own biometric identity, captured once, unrecoverable.

COPPA's exclusion of ByteDance and Mintegral SDKs from under-13 audiences exists for exactly this scenario: a company that knows, demonstrably, that its audience is children, and integrates advertising infrastructure not built or certified for that audience anyway.

Consumer Protection & Deceptive Design

Naming KidoZ and SuperAwesome as advertising partners, while the same binary carries eleven further, uncertified networks with a larger combined SDK footprint, functions as compliance theatre from a parent's perspective: the visible, checkable claim ("we use child-safe advertising") is true and simultaneously incomplete in a way that materially changes what a reasonable parent would decide. This is a deceptive-design pattern regardless of whether any individual store disclosure is technically false.

Article	Engaged by	Basis

Data Protection – Article by Article

Article	Engaged by	Basis
Art. 5(1)(a), 5(2)	Gap between the certified-partner narrative and the actual SDK footprint	Lawfulness, fairness, transparency; accountability
Art. 6, Art. 7	H2: 13 ad SDKs without a demonstrated consent mechanism	No documented lawful basis or consent flow for the non-certified networks
Art. 8	C1, C3: children's audience confirmed by the company's own parallel COPPA-certified integration	Parental consent requirement for children's data processing
Art. 9	C3: RECORD_AUDIO capturing children's voice	Special-category biometric data, no documented Art. 9(2) basis
Art. 13	Absence of plain-language disclosure naming Pangle/Mintegral alongside KidoZ/SuperAwesome	Transparency obligation toward the data subject (or their parent)
Art. 44-49	C2, C3: IMEI and voice-derived signal routed through three sequential China-bound infrastructure hops	International transfer without a documented Art. 46 safeguard

Platform Accountability & the DSA

Outfit7 is the first-party publisher and SDK integrator across all 17 titles; the findings in this report are the platform's own design choices, not third-party content requiring notice-and-takedown. Where any of these apps are distributed through app-store surfaces subject to the Digital Services Act's risk-assessment obligations for platforms serving minors, the coexistence of certified and uncertified child-facing advertising infrastructure documented here is directly relevant to that obligation.

Regulatory & Legal Landscape

Authority	Basis	Role in this case
Datenschutzbehoerde (DSB), Austria	GDPR Art. 8, 9, 44-49	BCC on R1, 2026-06-24
BfDI, Germany	GDPR Art. 8, 9, 44-49	BCC on R1, 2026-06-24
ICO, United Kingdom	UK GDPR Art. 8, 9	BCC on R1 – delivery blocked by a Microsoft mail-flow rule at the recipient's own infrastructure, confirmed 2026-06-24, not RFI-IRFOS's channel
CNIL, France	GDPR Art. 8, 9, 44-49	BCC on R1 – bounced, confirmed 2026-06-24, requires a verified alternative channel before any future correspondence
FTC (COPPA), United States	COPPA, 15 U.S.C. Sec.6501-6506	Not directly notified in this campaign; the ByteDance/Mintegral under-13 exclusion is a matter of established COPPA enforcement precedent, not a novel theory

Industry comparison: the specific pattern documented here – a certified children's-safe ad network integrated in parallel with, not instead of, ad-tech excluded from children's audiences – has not appeared in this form elsewhere in RFI-IRFOS's 2026 programme. Most children's-app findings in this corpus involve either the presence of inappropriate SDKs alone, or a certified-safe stack alone; the deliberate coexistence of both, at portfolio scale across 17 titles, is what elevates this case.

Indicators of Compromise / Reproducible Evidence

Item	Value
Primary analysed package	com.outfit7.talkingtom, version 5.1.3.3751 (code 200501030)
APK size	~92 MB
Pangle smali classes (Talking Tom Cat)	3,704
Mintegral smali classes (Talking Tom Cat)	3,268
RECORD_AUDIO code call sites (Talking Tom Cat)	117
Pangle IMEI endpoint (live example value)	union_imei=702f89a658bd1f189c6e8e24587cd9ce
Outfit7-owned China endpoints	aas-gapi.talkingtomandfriends.cn, apps2.outfit7.cn
Portfolio scope confirmed	17 titles, shared SDK signature

```
apktool d talkingtom_base.apk -o talkingtom_decoded
grep -r "union_imei" talkingtom_decoded/smali*/
grep -r "outfit7.cn\|talkingtomandfriends.cn" talkingtom_decoded/
grep -rl "RECORD_AUDIO" talkingtom_decoded/AndroidManifest.xml
```

Disclosure Timeline & Outcome

Date	Event
2026-06-24	R1 sent to dpo@outfit7.com, cc privacy@outfit7.com and xinyu.qian@outfit7.com, DSB/BfDI/ICO/CNIL in BCC. CNIL bounces; ICO blocked by a mail-flow rule on the recipient side.
2026-06-27	First follow-up, three days, no reply of any kind.
2026-07-02	Second follow-up, eight days since first contact, five since the first follow-up, cc widened to press@outfit7.com and the named regulators directly (not just BCC).
2026-07-17	Third follow-up.
2026-08-12	Fourth follow-up.

Date	Event
2026-08-21	Fifth follow-up.
2026-08-28	Sixth follow-up: sixty-five days of cumulative silence noted explicitly in the message itself.
2026-09-04	Seventh follow-up: seventy-two days, eight messages total, fifteen days stated to embargo, explicitly flagged as likely the last message before publication.
2026-09-11	Eighth follow-up: eighty-seven days, nine messages, zero replies of any kind – the final pre-publication notice.

The defining fact of this case

No other target in RFI-IRFOS's 2026 programme has produced nine written notices, across 87 days, with not one reply of any kind – not a denial, not an automated acknowledgment, not a bounce beyond the two regulator-address delivery failures on day one. The addresses are live. This is not a broken mailbox; it is a company that has read nine notices about a child's voice data routing to China and chosen, each time, not to answer.

Residual Risk & Recommendations

- None of the five findings has been confirmed addressed in any reply, because no reply has ever arrived.
- The RECORD_AUDIO → own-China-backend → Pangle → Mintegral chain (C3) remains, as far as RFI-IRFOS can verify externally, fully live across the portfolio.
- The ICO and CNIL delivery failures mean two of the four named regulators may not have received this disclosure through the channel used; both need a verified alternative contact before any further correspondence in this or related cases.
- For regulators: the COPPA exclusion of ByteDance and Mintegral from under-13 audiences is established precedent, not a novel legal theory RFI-IRFOS is proposing – Outfit7's own parallel use of certified alternatives is the evidentiary basis that the audience-knowledge element is already met.
- The binary will continue to be pulled and diffed weekly for the remainder of the embargo period across the full 17-title portfolio.

RFI-IRFOS's own view: a portfolio this size, generating this much revenue, from a company sophisticated enough to integrate two separate COPPA-certified ad networks correctly, does not fail to notice nine written notices about its own children's-app SDK stack. We read the silence as a decision, not an oversight, and we are naming that plainly rather than assuming good faith we have been given no evidence for. If that reading is wrong, the correction is simple: answer the three questions this disclosure has asked since 24 June. We will update the public record the moment that happens, on this case as on every other.

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 All findings derive from static root-level analysis of the publicly distributed application binaries using publicly available tooling. No servers, accounts, or backend infrastructure were probed. Technical evidence is archived under chain of custody and available to regulatory authorities on request. Research conducted under ISO/IEC 29147, the freedom of scientific research (Art. 17 StGG) and GDPR Art. 89. REF RFI-2026-OFT-001.