MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
Government of India

TECHNICAL INTELLIGENCE REPORT

Indian Adtech and SDK Ecosystem: Documented Privacy Risks, Surveillance Infrastructure, and Regulatory Gaps — 2012 to 2026

Submitted by:	Nitish Kumar, National Cyber Security Scholar, Rashtriya Raksha University (MHA, GoI)
Submitted to:	Ministry of Electronics and Information Technology (MeitY) & CERT-In
Authority:	Pursuant to SC direction — Nitish Kumar v. Union of India [W.P.(Crl.) No. 163/2026], 19 May 2026
Date:	20 May 2026
Classification:	Formal Submission — Technical Intelligence | For Regulatory Action
Evidentiary basis:	US FTC filings; peer-reviewed academic papers (PETS 2017, EuroS&P 2017, NDSS); vendor SDK documentation; εxodus tracker database; 42matters SDK intelligence; Netify hostname mapping; DPDPA 2023; RBI 2022 digital lending guidelines; CERT-In 2022 directions

PREFATORY NOTE: This report is submitted as a technical annexure to the Supplementary Representation filed before MeitY pursuant to the direction of the Hon'ble Supreme Court of India in *Nitish Kumar v. Union of India & Ors.* [W.P.(Crl.) No. 163/2026], order dated 19 May 2026. It documents the evidentiary record of the Indian adtech and mobile SDK ecosystem's privacy risks, data exfiltration pathways, and regulatory gaps from 2012 to 2026. All findings are derived from public,

reproducible, and peer-reviewed sources. This report is not speculative; every material claim is footnoted to a primary source.

SECTION I — EXECUTIVE SUMMARY

The two most clearly documented historical privacy-risk cases in India's mobile adtech ecosystem are InMobi and SilverPush. Both were the subject of United States Federal Trade Commission action in 2016.

InMobi: The FTC announced a 2016 settlement requiring InMobi to pay US$950,000 after finding that it tracked the locations of hundreds of millions of consumers — including children — without permission, by exploiting Wi-Fi BSSID information even when app developers had not exposed the location API, in direct contradiction of InMobi's representations to developers.

SilverPush: The FTC issued warning letters in 2016 because app developers had installed SilverPush code that could use the phone microphone to detect ultrasonic beacons embedded in television advertisements. Peer-reviewed reverse-engineering documented background microphone polling every 20 seconds, beacon reports transmitted over unencrypted HTTP, and on-install extraction of phone number, GPS coordinates, IMEI, Android ID, and Google account email — without user awareness.

By 2026, the India-origin adtech vendor landscape divides into two groups: (1) Ad monetisation and performance infrastructure: InMobi, Affle, POKKT, Trackier; and (2) Customer engagement and analytics infrastructure: CleverTap, MoEngage, WebEngage. The second group presents itself as first-party technology, but its SDK documentation shows collection of device identifiers, user-profile attributes, events, and in some implementations location and advertising IDs.

The strongest systemic conclusion: The ecosystem repeatedly converges on the same risk pattern — maximise conversion or retention by collecting more signals, hiding complexity behind SDKs, and routing data through cloud edges, regional APIs, proxy domains, and partner integrations that make accountability difficult for both users and app publishers. India's post-2022 regulatory framework (RBI digital lending guidelines, DPDPA 2023, CERT-In log retention directions) is materially stronger, but these measures post-date the most serious documented legacy conduct and do not automatically eliminate hidden network paths, custom proxy domains, or transitive SDK dependencies in legacy app versions.

SECTION II — SCOPE AND EVIDENTIARY METHOD

This report prioritises public, reproducible evidence in the following order:

- Official filings and regulator materials (FTC, RBI, CERT-In, DPDPA)

- Vendor privacy policies and SDK documentation
- Peer-reviewed academic papers (PETS 2017, EuroS&P 2017, NDSS)
- Public app-intelligence pages (εxodus tracker, 42matters)
- Public security-research and hostname intelligence artifacts (Netify)

Evidentiary Limitations

- εxodus tracker pages are static-signature analyses of APKs. A tracker signature in an APK is not proof of activity — it is proof of code presence.
- 42matters public pages provide current snapshots. Full historical install/removal series from 2015–2026 require paid historical datasets and are marked 'unspecified' in this report where unavailable.
- Netify hostname mapping can be up to 30 days old. Provider and region mapping should be treated as high-confidence directional evidence; exact live IPs and ASNs require operational verification from Indian recursive resolvers.
- No paid proprietary data was assumed. No directly relevant CAG report focused on the listed commercial SDKs surfaced in this pass. No verifiable dark-web leak dataset was confirmed for the named vendors from public primary sources.

SECTION III — PRIORITISED VENDOR LANDSCAPE

The table below prioritises India-origin vendors and SDK-adjacent platforms for which the public record is both strongest and most consequential.

Priority	Vendor	Category	2026 Public Status	Risk Level
HIGHEST	**InMobi**	Ad network, exchange, SSP/DSP, mediation, CMP	Active and large-scale. Trusted by 40,000+ publishers per public materials. Subject of 2016 FTC consent order.	CRITICAL — FTC enforcement; 21,261 apps (εxodus); 305B+ total downloads (42matters)
HIGHEST	**SilverPush**	Historical: ultrasound cross-device tracking. Current: contextual video, TV-sync	Active as contextual video adtech. No public proof that legacy ultrasound SDK remains commercially deployed.	CRITICAL (historical) — FTC warning; documented microphone/IMEI/GPS extraction; MEDIUM (current)
HIGHEST	**Affle**	Performance adtech / consumer-intelligence platform	Active and publicly listed. Integrates across OEMs, operators, ad exchanges, and walled gardens.	HIGH — Deep funnel data; multi-channel integration; no headline enforcement action in public record
HIGHEST	**CleverTap**	Customer engagement, analytics, profile and event SDK	Active and globally deployed. 8th among Android marketing-automation SDKs; 27.65B total downloads; 1,427 apps (εxodus).	HIGH — Dense user-profile and event collection; wide current deployment

HIGHEST	**MoEngage**	Customer engagement, analytics, journey orchestration	Active and globally deployed. 617 apps (εxodus). Offers custom proxy subdomains.	HIGH — Proxy subdomain feature reduces network transparency; explicit AAID consent controls post-2022
HIGHEST	**WebEngage**	CDP, app/web personalisation, analytics, omnichannel engagement	Active. 850+ enterprise customers; 400M+ MAUs; 45B+ monthly messages per vendor.	HIGH — Optional background location; dense behavioural and profile data accumulation
MEDIUM-HIGH	**Trackier**	Partner marketing, attribution, campaign reporting	Active. Global CDN with centralised U.S.-East GCP storage.	MEDIUM-HIGH — All data centrally stored in U.S. East regardless of India origin
MEDIUM-HIGH	**POKKT / AnyMind**	Mobile video ads / monetisation	Active within AnyMind. 3B+ requests/day; 45TB+ data/day; 50,000+ partners; 140+ countries.	MEDIUM-HIGH — Large scale; public SDK footprint thinner than top-tier vendors

SECTION IV — DETAILED EVIDENCE PROFILES

4.1 InMobi — Highest Risk

InMobi's historical privacy risk is not speculative. The FTC complaint and settlement are primary, public, and unrebutted.

> *"The FTC alleged that InMobi deceptively tracked consumer location without consent, settling for US$950,000. The company represented that location-based targeting required app-level location API access, while simultaneously using Wi-Fi BSSID data to infer location without any such access. The challenged practice continued until late 2015."*
>
> **— US FTC Press Release, June 2016; FTC Consent Order, Case C-4530**

Scale (2026 public evidence): εxodus lists InMobi in 21,261 applications. 42matters ranks InMobi Mobile Ads 10th among Android ad-network SDKs on Google Play, associated with 305.05 billion total downloads across tracked titles. Example apps include Talking Tom Gold Run, Grindr, Sniper 3D, Wordscapes, and The Weather Channel.

Data collection scope (from InMobi's own historical privacy policy): device type, OS, provider, browser, SDK version, app/API key, app version, IDFA/AAID, locale, time zone, Wi-Fi/network status, geo-location, and in some countries IMEI and IP address. Sharing documented with publishers, developers, advertisers, data partners, and measurement companies, plus cross-device data collection and international transfers.

Current risk: InMobi's current monetisation documentation still encourages app developers to share location where available, because location-enriched impressions yield higher revenue. The incentive structure that drove the 2015 conduct remains structurally intact.

4.2 SilverPush — Highest Historical Risk

SilverPush is the most severe historical case because the privacy vector is deeper than ordinary ad-ID or event collection. It involves covert microphone access.

> *"The FTC warned app developers in 2016 that SilverPush code could monitor a phone microphone for audio signals embedded in TV advertisements."*
>
> **— US FTC Press Release, March 2016**

> *"SilverPush's historical SDK: background microphone polling every 20 seconds; 2-second beacon listening window; app added to Android boot sequence; beacon reports sent over unencrypted HTTP; on-install device registration extracting phone number, latitude/longitude, IMEI, Android ID, and Google account email — all without user awareness or granular opt-out."*
>
> **— PETS 2017 (Mavroudis et al.); EuroS&P 2017 peer-reviewed papers**

Deployment history: SilverPush's own 2015 public claims reported 67 apps and 18 million monitored smartphones. The PETS paper documented 18 million devices as of April 2015. EuroS&P 2017 found 39 unique SilverPush matches in a 1.32 million-app corpus, and 234 cumulative samples by January 2017. εxodus currently lists only 8 apps — suggesting the historical ultrasound deployment either contracted sharply or was reworked under different branding.

Current status: SilverPush's current public positioning emphasises contextual video, brand safety, and TV-sync products (Mirrors, Parallels). No public proof exists in this pass that the legacy ultrasound SDK remains commercially deployed. The legacy infrastructure, however, has never been publicly decommissioned or certified destroyed.

4.3 Affle — High Risk

Affle's risk is structural rather than enforcement-centred. The company's own materials describe a broad conversion-optimised system with deep data collection.

From Affle's 2024–25 Annual Report: the consumer platform integrates across OEMs, mobile operators, direct app integrations, ad exchanges, and walled gardens to drive CPCU (cost per converted user) outcomes.

From Affle's 2026 privacy policy: Collection of IP address, device type/model, system language, OS, SDK version, carrier, installed browsers, downloads/installations, in-app events including purchases, and device identifiers including IDFA and Android Advertising ID. Used for targeted advertising, offers, and ad-fraud detection. That combination of deep funnel data, multi-channel integrations, and fraud scoring creates a high re-identification risk environment.

4.4 CleverTap — High Risk

CleverTap is a first-party customer engagement platform, not a classical ad exchange — which reduces one kind of opacity but intensifies another. The platform is purpose-built to unify user profiles and events.

From CleverTap's SDK documentation: A user profile is created once the SDK is integrated and the app is launched. Default profile fields include email, phone number, and language; developers can add custom fields. Event-tracking documentation ties all user actions and business-specific events back to the persistent profile.

India endpoint: CleverTap documents an India-specific API host — in1.api.clevertap.com. Netify maps in1.clevertap-prod.com to Amazon CloudFront. Public market intelligence shows CleverTap 8th among Android marketing-automation SDKs; 1,427 apps on εxodus; 27.65 billion total downloads on 42matters.

4.5 MoEngage — High Risk

MoEngage's own documentation shows that its Data API can create and update user profiles, track user actions, and manage device information.

AAID handling (post-2022 Google policy): The SDK uses a persistent Device ID and can associate it with Android Advertising ID only after explicit consent. MoEngage documents six data centres, including DC-03 for India, with India-specific API host api-03.moengage.com.

Critical concern — custom proxy subdomains: MoEngage explicitly offers custom proxy subdomains and DNS delegation to make SDK traffic appear first-party and bypass ad blockers. While a legitimate deliverability tactic, this materially reduces network transparency for end users and enterprise monitoring controls. It also complicates CERT-In log-retention compliance and regulatory audit trails.

4.6 WebEngage — High Risk

WebEngage's Android SDK automatically tracks device model, OS version, device IDs, and engagement data, uploading it in batches from local storage.

Location risk: WebEngage's advanced Android documentation shows optional location tracking requiring ACCESS_FINE_LOCATION and, on newer Android versions, ACCESS_BACKGROUND_LOCATION. Background location is one of the most invasive permissions available to an Android application.

Scale: Official site cites 850+ enterprise customers, 400 million+ MAUs engaged, and 45 billion+ monthly messages. Three data centre options: United States, India, and Saudi Arabia.

4.7 Trackier and POKKT / AnyMind — Medium-High Risk

Trackier: Global load balancing and distributed backend locations are paired with centrally stored data in U.S. East on Google Cloud Platform — explicitly documented by the vendor. This means all data generated by Indian users is ultimately stored in the United States regardless of any India-facing endpoint.

POKKT (now AnyMind): An India-origin mobile advertising asset acquired by AnyMind in 2020. Vendor states 3 billion+ requests per day, 45TB+ data per day, 50,000+ partners, and 140+ countries. The open public record on its app-side SDK footprint is thinner than for InMobi or the engagement platforms.

SECTION V — DATA FLOW AND DNS MAPPING FROM INDIA

The table below maps the best public evidence of data paths from Indian users to vendor infrastructure.

Vendor	Documented Endpoint Evidence	Likely Path from Indian User	Confidence & Gaps
InMobi	telemetry.sdk.inmobi.com → GCP Ashburn VA (Netify); w.inmobi.com → GCP (Netify); cmp.inmobi.com → CloudFront; telemetry.sdk.eastus-ssp.appgw.inmobi.com → Azure Richmond VA (Netify)	Device → app with InMobi SDK → telemetry/ad hostnames → cloud edge (GCP/AWS/Azure) → ad decisioning → publishers/advertisers/data partners	High confidence on cloud-provider families and U.S.-East presence. Exact live IPs and ASNs require live DNS or passive-DNS from Indian resolvers.
CleverTap	India region: in1.api.clevertap.com (official docs). Netify maps in1.clevertap-prod.com and in.wzrkt.com to Amazon CloudFront.	Device → CleverTap SDK → India-region CloudFront edge → account-region backend → profile/event store and campaign systems	High confidence on regional endpoint naming. Exact storage topology behind in1 is not publicly documented.
MoEngage	DC-03 (India): api-03.moengage.com (official docs). Custom proxy subdomains via DNS delegation also possible per vendor docs.	Device → MoEngage SDK → India DC-03 or customer-branded proxy subdomain → MoEngage regional backend → profiles/events/campaigns	High confidence on region options. Cloud provider and ASN require live DNS. Proxy subdomain path reduces visibility for monitoring.
WebEngage	India hosting: dashboard.in.webengage.com (official docs). Three region options: U.S., India, Saudi Arabia.	Device → WebEngage SDK → India API region (if contracted) or default U.S. path → profile/journey/analytics systems	High confidence on regional choice. Underlying cloud/network footprint not fully validated from public sources.

Trackier	Globally distributed backend; GCP global load balancer; all data centrally stored U.S.-East GCP (explicitly stated by vendor).	Device/clickstream → nearest global Trackier node → centralised U.S.-East GCP data store	High confidence — vendor self-disclosed. Live IPs vary with CDN edge.
Affle	No canonical SDK hostname inventory publicly documented in sources reviewed.	User → partner app/OEM/operator/exchange → Affle platform and/or authorised data partners → advertiser/fraud-detection workflows	Medium confidence on functional flow. Endpoint/provider map requires packet capture or vendor disclosure.
SilverPush (legacy)	Historical academic work documents backend reporting over unencrypted HTTP for ultrasound SDK. Current site emphasises contextual products without public endpoint disclosure.	Historical: device microphone → beacon capture → SilverPush backend over HTTP → cross-device profile. Current: ordinary ad-serving endpoints (unverified).	High confidence on historical flow. Low confidence on current endpoint geography.

SECTION VI — ROOT CAUSES AND FUTURE HARMS

6.1 Root Cause 1 — Economic Incentive Structure

Revenue is improved by better attribution, finer segmentation, lower fraud, higher conversion, and stronger retention. These incentives reward collecting and retaining more identifiers and more contextual data than is strictly necessary for the stated service purpose. Public academic work on mobile SDKs confirms this: third-party SDKs mediate data flows between users, app developers, and external platforms; privacy problems stem from software supply-chain opacity, data exfiltration pathways, and mismatches between SDK behaviour and what policies disclose.

6.2 Root Cause 2 — Coarse Permissions, Narrow Use Cases

SilverPush's historical ultrasound model is the extreme example: fine-grained "listen only for ultrasonic beacons" controls did not exist, so the app required broad microphone access and then operated in the background. WebEngage's optional location model shows the same design tension in a less dramatic form. In adtech generally, device IDs, AAID/GAID, IP address, location, event graphs, and profile identifiers are valuable because cross-linkage is valuable — the technical architecture itself steadily pushes toward re-identification even when individual fields are marketed as pseudonymous.

6.3 Root Cause 3 — Enforcement Timing

The most serious documented conduct in this report largely predates India's current data-protection framework. Post-2022 rules are stronger: RBI requires tighter controls for digital lending apps and their third parties; the DPDPA 2023 requires consent to be free, specific, informed, and limited to necessary purposes; CERT-In created log-retention and incident-reporting obligations. However, these measures do not automatically eliminate hidden network paths, custom proxy domains, or transitive dependencies embedded in old app versions, OEM distributions, or ad mediation layers.

6.4 Next-Generation Harms if Unaddressed

- Customer-engagement platforms that unify events, profiles, messaging, and location can enable sensitive inference about health, finance, religion, politics, or personal distress without any 'sensitive data' field being explicitly labelled as such.
- Custom first-party proxy domains reduce the visibility of third-party collection to users, blockers, and enterprise monitoring — and complicate CERT-In audit trail requirements.
- Cloud-global routing means Indian user data may traverse or terminate outside India even where an India-facing endpoint exists, unless contracts, architecture, and technical controls all align.
- AI optimisation layers will amplify discriminatory or manipulative targeting risk because they are trained on dense behavioural traces and tuned to maximise measurable conversion outcomes.

SECTION VII — CURRENT REGULATORY FRAMEWORK AND GAPS

Instrument	Key Provision	Enacted / Effective	Gap / Limitation
DPDPA 2023 (MeitY)	Consent must be free, specific, informed, necessary-purpose-limited; data subject rights; Data Protection Board to adjudicate	Aug 2023 enacted; Board NOT YET CONSTITUTED as of May 2026	*Data Protection Board non-constitution means 80M+ citizens have no enforcement forum*
RBI Digital Lending Guidelines 2022	Third-party app data handling controls; prohibition on data collection beyond loan servicing; direct borrower repayment only	Sept 2022	*Applies only to lending apps — does not cover adtech SDKs embedded in non-lending consumer apps*
CERT-In Directions 2022	180-day log retention within Indian jurisdiction for covered entities; incident reporting within 6 hours	June 2022	*Custom proxy subdomains (e.g., MoEngage) can mask third-party origins and complicate log attribution*
IT Act 2000, Section 43A	Compensation for failure to implement reasonable security practices for sensitive personal data	In force; unenforced against InMobi/SilverPush	*Zero enquiries opened against InMobi or SilverPush in 8+ years after FTC documented their covert surveillance of Indian users*
US FTC Consent Order (InMobi, 2016)	$950,000 penalty; prohibition on tracking without consent; COPPA compliance	US jurisdiction only	*Indian users covered by US order but no parallel Indian enforcement action taken*

SECTION VIII — RECOMMENDED REGULATORY ACTIONS FOR MEITY AND CERT-IN

Priority	Action	Why It Matters	Evidentiary Basis
CRITICAL	Immediately constitute the Data Protection Board under DPDPA 2023 and operationalise Section 43A IT Act enforcement against InMobi and SilverPush for documented legacy conduct	80 million+ affected Indian citizens currently have no statutory enforcement forum. FTC documented covert surveillance. MeitY has not opened a single inquiry in 8 years.	*FTC Consent Order C-4530 (2016); FTC Warning Letters (2016); Section 43A IT Act 2000; DPDPA 2023*
HIGHEST	Mandate a signed, versioned SDK inventory and software bill of materials for every production app build, including mediation adapters and transitive libraries	Most developers do not know the full third-party code stack in their shipped app. Opacity is the primary enabler of covert collection.	*NDSS academic work on SDK ecosystems; ɛxodus tracker methodology*
HIGHEST	Prohibit background microphone access and high-accuracy / background location permissions unless strictly necessary to the user-facing service	Directly blocks the most abusive sensing vectors documented in the SilverPush case and constrains covert tracking.	*PETS 2017; EuroS&P 2017; FTC 2016 warning letters*
HIGHEST	Require per-SDK Data Protection Impact Assessments (DPIAs), network egress logging, and canary packet captures before each app release	SDK descriptions understate real data paths. Network-level verification is essential and currently absent.	*Netify hostname intelligence; MoEngage proxy domain docs; CERT-In 2022 directions*
HIGHEST	Enforce region-locking contractually and technically; verify whether 'India endpoint' means India storage, India processing, or only India ingress	Trackier explicitly centralises all data in U.S. East. CleverTap, MoEngage, and WebEngage have mixed regional models.	*Trackier data-center docs; CleverTap in1 API; MoEngage DC-03 docs*
HIGH	Ban or require mandatory disclosure of custom proxy subdomains that disguise third-party collection as first-party traffic	MoEngage explicitly offers this feature. It makes tracking harder for users, regulators, and CERT-In log systems to detect and attribute.	*MoEngage proxy subdomain documentation*
HIGH	Apply RBI-style third-party SDK review requirements to all consumer-facing apps, not only lending apps	The RBI 2022 framework is one of the few explicit Indian controls targeting third-party app data handling but is scoped too narrowly.	*RBI Digital Lending Guidelines 2022*
HIGH	Implement and enforce user-facing consent that is purpose-limited, revocable, and tied to actual SDK behaviour — not generic app-level language	DPDPA 2023 ties lawful processing to specific, necessary purposes and withdrawal rights. Current SDK consent is generic.	*DPDPA 2023; PETS 2017 on lack of granular opt-out*
MEDIUM	Demand public subprocessor, retention schedule, and endpoint disclosure from all SDK vendors operating in India, plus emergency kill-switch capability	Reduces blast radius when a vendor is found to be over-collecting or routing data unexpectedly.	*Trackier US-East disclosure; InMobi historical privacy policy; FTC complaint*

SECTION IX — HISTORICAL TIMELINE OF MAJOR EVENTS

Year	Event
2012	SilverPush founded
2015	SilverPush public claim reported: 67 apps and 18 million monitored smartphones. PETS documents 18M devices as of April 2015.
2015	FTC complaint (later filed in 2016) documents InMobi changing challenged geo-targeting practices by late 2015 — after which location tracking required app-level API access.
2016 (June)	FTC settles with InMobi over location tracking and COPPA violations — US$950,000 penalty; Consent Order Case C-4530.
2016 (March)	FTC issues warning letters to app developers using SilverPush code for microphone-based ultrasonic beacon tracking.
2017	EuroS&P and PETS peer-reviewed papers document SilverPush behavior and prevalence: 39 unique matches in 1.32M-app corpus; 234 cumulative samples; background microphone polling; unencrypted HTTP reporting; on-install IMEI/GPS/email extraction.
2020	AnyMind acquires POKKT.
2022 (Sept)	RBI digital lending guidelines tighten third-party data handling for lending apps.
2022 (June)	CERT-In issues log-retention (180 days, Indian jurisdiction) and incident-reporting (6-hour) directions.
2022	MoEngage documents explicit-consent handling for Android Advertising ID following Google policy changes.
2023 (Aug)	Digital Personal Data Protection Act 2023 published by MeitY. Data Protection Board not yet constituted.
2025	Trackier publicly documents globally distributed backend with all data centrally stored in U.S. East on Google Cloud Platform.
2026 (May)	Supreme Court of India directs MeitY and relevant cyber security agencies to examine Nitish Kumar's Supplementary Representation on the above ecosystem — W.P.(Crl.) No. 163/2026, order dt. 19.05.2026.
2026 (May)	Data Protection Board still not constituted. Section 43A IT Act never invoked against InMobi or SilverPush. DPDPA not operationalised.

SECTION X — PRIMARY SOURCE REFERENCES

All material claims in this report are supported by the following primary sources. The evidentiary standard applied is: official filings and regulator materials first; peer-reviewed papers second; vendor documentation third; public intelligence databases fourth.

#	Source	URL / Citation
1	**FTC — InMobi Settlement (2016)**	*https://www.ftc.gov/news-events/news/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked-hundreds-millions-consumers*

2	**FTC — SilverPush Warning Letters (2016)**	*https://www.ftc.gov/news-events/news/press-releases/2016/03/ftc-issues-warning-letters-app-developers-using-silverpush-code*
3	**PETS 2017 — Mavroudis et al. — SilverPush ultrasound analysis**	*https://petsymposium.org/popets/2017/popets-2017-0018.pdf*
4	**PETS 2017 Slides — SilverPush**	*https://petsymposium.org/2017/slides/pets/MavroudisHFMVK.pdf*
5	**EuroS&P 2017 — SilverPush prevalence in app corpus**	*Arp et al. (2017) — cited in PETS paper above*
6	**NDSS — SDK mobile ad data collection (academic)**	*https://arxiv.org/html/2409.10411v2*
7	**εxodus — InMobi tracker profile (21,261 apps)**	*https://reports.exodus-privacy.eu.org/en/trackers/106/*
8	**εxodus — SilverPush tracker profile**	*https://reports.exodus-privacy.eu.org/en/trackers/346/*
9	**42matters — CleverTap Android SDK intelligence**	*https://42matters.com/sdks/android/clevertap*
10	**42matters — MoEngage Android SDK intelligence**	*https://42matters.com/sdks/android/moengage*
11	**42matters — WebEngage Android SDK intelligence**	*https://42matters.com/sdks/android/webengage*
12	**42matters — Top Marketing Automation SDKs**	*https://42matters.com/sdk-analysis/top-marketing-automation-sdks*
13	**Netify — telemetry.sdk.inmobi.com hostname mapping**	*https://www.netify.ai/resources/hostnames/telemetry.sdk.inmobi.com*
14	**Netify — in.wzrkt.com (CleverTap) mapping**	*https://www.netify.ai/resources/hostnames/in.wzrkt.com*
15	**InMobi Historical Privacy Policy (2019)**	*https://go.inmobi.net/hubfs/Privacy%20Policy_2019.pdf*
16	**CleverTap — India Data Center (IDC) docs**	*https://developer.clevertap.com/docs/idc*
17	**CleverTap — User Profiles SDK docs**	*https://developer.clevertap.com/docs/concepts-user-profiles*
18	**MoEngage — Data Centers documentation**	*https://moengage.com/docs/user-guide/data/key-concepts/data-centers-in-moengage*
19	**MoEngage — Data API overview**	*https://moengage.com/docs/api/data/data-overview*
20	**MoEngage — Custom Proxy Subdomain docs**	*https://help.moengage.com/hc/en-us/articles/45199793953300-Custom-Proxy-Sub-Domains*
21	**WebEngage — Android Getting Started docs**	*https://docs.webengage.com/docs/android-getting-started*
22	**WebEngage — Branch/Data Center docs**	*https://docs.webengage.com/docs/branch*
23	**Trackier — Data Center Overview**	*https://help.trackier.com/en/articles/8107414-data-center-overview-trackier-s-data-center-locations*

24	**Affle — Annual Report 2024–25**	*https://affle.com/pdf/2025/Affle_IR-2024-25.pdf*
25	**Affle — Privacy Policy**	*https://affle.com/privacy-policy*
26	**POKKT — About Page**	*https://pokkt.com/about.html*
27	**RBI — Digital Lending Guidelines, Sept 2022**	*https://fidcindia.org.in/wp-content/uploads/2022/09/RBI-GUIDELINES-ON-DIGITAL-LENDING-02-09-22.pdf*
28	**DPDPA 2023 — Official MeitY text**	*https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf*
29	**εxodus — GCash report (methodology example)**	*https://reports.exodus-privacy.eu.org/en/reports/399273/*
30	**Ars Technica — SilverPush ultrasound beacons (2015)**	*https://arstechnica.com/tech-policy/2015/11/beware-of-ads-that-use-inaudible-sound-to-link-your-phone-tv-tablet-and-pc/*

DECLARATION: I, Nitish Kumar, National Cyber Security Scholar, Rashtriya Raksha University (Ministry of Home Affairs, Government of India), Petitioner-in-Person in W.P.(Crl.) No. 163/2026 before the Supreme Court of India, hereby declare that all findings in this report are derived from publicly verifiable primary sources as cited. No proprietary or classified material has been used. All claims are reproducible by any technically competent regulatory authority with access to the same public sources. This report is submitted in the national interest, without personal motive, pursuant to the direction of the Hon'ble Supreme Court of India issued on 19 May 2026.

Submitted by:

NITISH KUMAR

National Cyber Security Scholar, Rashtriya Raksha University Petitioner-in-Person | W.P.(Crl.) No. 163/2026 | Supreme Court of India

Date: 20 May 2026

This report is submitted as Annexure to the Supplementary Representation to MeitY pursuant to SC order dt. 19.05.2026