MOBILE SURVEILLANCE ARCHITECTURE

Audio Beacons | AI Vision | AdTech RTB | Android Permissions | China Data Mirroring

Complete Technical Architecture Report — 2017 to 2026

CONFIDENTIAL RESEARCH | April 2026

TABLE OF CONTENTS

1. ULTRASONIC AUDIO BEACON ARCHITECTURE

1.1 What Are Ultrasonic Audio Beacons?

Ultrasonic audio beacons are inaudible high-frequency tones embedded into audio content — TV advertisements, radio broadcasts, retail store audio systems, website JavaScript, and even in-app audio — operating in the 18 kHz to 22 kHz frequency range. The human ear cannot detect sounds above approximately 18 kHz (and most adults over 30 cannot hear sounds above 16 kHz). Mobile phones, however, can record frequencies up to 22 kHz or higher using standard microphone hardware.

When a mobile app with the RECORD_AUDIO permission is installed and running — or listening in the background — it can detect these ultrasonic tones and decode the embedded data without the user's knowledge. The technique is called Ultrasonic Cross-Device Tracking (uXDT).

1.2 Complete Technical Architecture

Step 1: Beacon Emission Sources

Ultrasonic beacons can be emitted from multiple sources simultaneously:

- Television advertisements: A beacon is encoded into the audio track of the commercial. Any device nearby with a compatible app hears it.
- Retail store speakers: Physical ultrasonic emitters installed at store entrances. Found in 4 of 35 stores tested in two European cities (Braunschweig Technical University, 2017).
- Website JavaScript: A webpage plays an ultrasonic tone through the browser's Web Audio API when loaded. SilverPush used this to link desktop cookies to mobile device IDs.
- Radio broadcasts: Ultrasonic beacons embedded in radio ad streams.
- In-app audio: Beacons played within one app to be detected by another app on the same device.

Step 2: The SilverPush SDK Architecture (Primary Implementation)

The SilverPush SDK was the dominant ultrasonic tracking technology from 2014 to 2017. Its architecture was documented by researchers from Braunschweig Technical University and confirmed by FTC investigations.

Component	Technical Detail	What It Does
SDK integration	Added to app's codebase, typically 50-200KB	Developer adds SilverPush SDK to their app (flashlight, game, utility) — often without full understanding of its scope
RECORD_AUDIO permission	Requests RECORD_AUDIO in AndroidManifest.xml	Grants SDK access to continuous microphone stream even when app is backgrounded
Sampling rate	44,100 Hz audio sampling	Standard audio sampling rate — captures human speech AND ultrasonic range 18-22kHz simultaneously

Frequency analysis	FFT (Fast Fourier Transform) on 4,096-sample audio blocks	Decomposes captured audio into frequency components to detect beacon patterns
Beacon detection	Pattern matching at 18-20 kHz range	Identifies specific frequency signatures embedded by SilverPush advertisers
Device linking	Transmits beacon ID + Android device GAID/IMEI to SilverPush server	Links the detected beacon (e.g. from a specific TV ad) to the specific mobile device
Cross-device graph	SilverPush server correlates beacon events with desktop cookies	Determines that your phone and your laptop belong to the same person without any account login
Data output	User profile: TV viewing history, location, device graph	Sold to advertisers for targeting — or broadcast via RTB bidstream

Step 3: Three Commercial SDK Implementations

SDK / Company	Tracking Type	Technical Method	Apps Using It	Disclosed?
SilverPush (India, 2014)	Cross-device TV tracking	Detects beacons in TV ads via mic; links to desktop cookie; 44.1kHz sampling; FFT analysis	234+ Android apps by 2017; 18M+ devices; McDonald's and Krispy Kreme (Philippines) — since removed	NO — not disclosed to users
Lisnr (USA, 2012)	Physical location tracking	Ultrasonic beacons in retail stores; confirmed presence in 4/35 European stores tested	Retail and ticketing apps; now used in contactless payments (Mastercard partnership)	Partially — store-level disclosure only
Signal360 / Walkbase	Event / venue tracking	Ultrasonic beacons at sports venues; SDK in NBA team apps (Golden State Warriors, Sacramento Kings)	Golden State Warriors app, Sacramento Kings app — class-action filed 2016	NO — not disclosed; lawsuit followed
Shopkick	Retail rewards tracking	Ultrasonic emitters at Best Buy, Macy's; app detected entry; rewarded users with points	Shopkick app (reward-based so partially disclosed)	YES — reward mechanism means users know

WARNING: CRITICAL CAPABILITY: Since the SilverPush SDK records at 44,100 Hz — the full audio spectrum — it technically captures all audible human speech, not just ultrasonic beacons. SilverPush claimed it only analyzes the ultrasonic range, but independent security researchers confirmed the full audio data is temporarily stored during analysis, with no external audit of what actually gets processed or retained.

Step 4: Tor Deanonymization via Ultrasonic Beacons (2016)

In November 2016, researchers from University College London, UC Santa Barbara, and Politecnico di Milano demonstrated at Black Hat EU that ultrasonic beacons could deanonymize Tor users. The attack works as follows:

- A Tor user visits a malicious or compromised website that plays an ultrasonic beacon through JavaScript Web Audio API or a Flash element.
- The Tor user's phone, if nearby and running an app with RECORD_AUDIO access and the beacon detection code, picks up the ultrasonic tone.
- The phone sends its GAID, IMEI, GPS coordinates, and the beacon ID to the tracking server.
- The server now has both the Tor session (from the website visit) and the phone's real IP address and identity — the anonymity is broken.
- A state-sponsored actor could subpoena the advertiser and obtain the real user's identity, IP address, geolocation, IMEI, and more.

Step 5: FTC Intervention and SDK Evolution (2016–Present)

Year	Event	Technical Change	Current Status
2014	SilverPush launches Unique Audio Beacon product; Procter & Gamble and LINE among first clients	SDK deployed in 67 apps by April 2015; 18M devices affected	Active
2015	Citizen Lab and academic researchers document uXDT in research papers	First public technical analysis of 44.1kHz FFT beacon detection architecture	Exposure begins
2016 March	FTC sends warning letters to 12 app developers using SilverPush SDK	FTC states: 'code is configured to access microphone even when app is not in use'	Regulatory action
2017 May	Braunschweig researchers find 234 Android apps using ultrasonic tracking	Apps include games, utilities, news apps — most users unaware	Major exposure
2017	Google removes identified apps from Play Store	234 apps either suspended or updated to remove SDK	Platform enforcement
2019	SilverPush relaunches as Mirrors — AI-powered in-video ad targeting	Pivoted to computer vision: analyzes video content being viewed; no longer ultrasonic	Rebranded but alive

2020	LISNR pivots to contactless payments (Mastercard partnership)	Ultrasonic data transmission now used for payment verification at POS terminals	Active in payments
2022+	Ultrasonic beacons used in IoT, retail analytics, interactive displays	Technology migrated from advertising to infrastructure — harder to regulate	Active, less visible
2026	Kaspersky reports record Android attacks; new attack vectors via NFC relay and banking trojans	Ultrasonic tech merged into broader acoustic attack surface	Ongoing threat

2. AI VISION / COMPUTER VISION HARVESTING ARCHITECTURE

2.1 How Apps Use Camera Permission for More Than Photos

The CAMERA permission on Android and iOS grants an app access to the device's camera hardware and its live video feed. Apps with legitimate use cases — QR scanners, video call apps, AR filters — use this permission openly. However, the same permission is also used by apps to run continuous computer vision analysis in the background, harvesting biometric data without user awareness.

2.2 The AI Vision Pipeline Architecture

Stage 1: Camera Capture

Apps access camera frames at rates from 5 fps (low power background monitoring) to 60 fps (real-time face tracking). Even at 5 fps, 300 frames per minute are analyzed. Face++ SDK (China-based Megvii) can process 106 facial landmarks per frame. At 5 fps, this produces 31,800 facial data points per minute.

Stage 2: On-Device Processing

Modern AI vision SDKs perform processing on-device using TensorFlow Lite, Core ML (Apple), or proprietary neural network models. This means the raw camera feed never leaves the device — but the extracted biometric data (facial geometry, emotion scores, attention metrics) is transmitted to remote servers.

SDK / Platform	Developer	Facial Landmarks	Data Extracted	Where It Goes
Face++ / Facepppp	Megvii, Beijing, China	106 per frame	Facial geometry, age, gender, emotion, ethnicity, beauty score, glasses, accessories	Megvii servers, China — law enforcement in China has documented access
ARKit (Apple)	Apple, USA	52 blend shapes per frame	Facial expression map, head pose, eye gaze direction, tongue detection	On-device by default; app can upload if permitted
ML Kit Face Detection	Google	468 facial landmarks	Face mesh geometry, head pose, iris position	On-device; may sync to Google servers depending on app implementation
Banuba Face AR SDK	Banuba, Belarus/USA	84 landmark points	Facial geometry for AR filters; can extract age/gender estimates	App-controlled; used in Snap, TikTok, various beauty apps

Agora (AgoraIO)	Agora, China-origin	N/A (video)	Full video stream processing; call participants' faces accessible to Agora servers	Agora cloud servers; company has China ties

Stage 3: Biometric Data Monetisation

The extracted biometric data follows several monetisation paths:

- Direct sale to data brokers: Facial geometry data sold as part of user profile packages. Clearview AI built a 30+ billion image facial recognition database using publicly scraped images combined with facial data from apps.
- Model training: Millions of face scans train commercial facial recognition AI. The resulting model is licensed to governments, law enforcement, and retailers as a subscription service — you trained the model for free.
- Advertising targeting: Emotion AI (detecting whether a user looks interested, confused, or happy) is used in RTB bid requests as a targeting signal. Advertisers pay a premium for 'engaged' users.
- Identity verification products: Facial geometry databases are used to build KYC (Know Your Customer) verification services sold to banks and financial institutions.

2.3 Specific App Categories Using AI Vision Harvesting

App Category	Stated Purpose	Actual AI Vision Usage	Data Harvested	Examples
Beauty / Selfie filters	Beautify photos	Full facial geometry mapping; ethnicity/age/gender classification; emotion detection	468 landmarks, facial geometry hash, demographic estimates	BeautyPlus (Meitu, China), SNOW, YouCam Makeup
AR 'try-on' apps	Try glasses, makeup, clothes	3D facial mesh; head dimensions; skin tone analysis	Facial structure, head dimensions — usable for 3D face model reconstruction	Sephora Virtual Artist, Warby Parker, various fashion apps
Dating apps with photo AI	Profile photo enhancement	Face attractiveness scoring; facial similarity matching; age verification	Facial geometry, attractiveness scores, identity verification biometric	Various — some apps use Face++ attractiveness API
Deepfake AI apps	Create AI video effects	Full facial capture; expression mapping; voice cloning together	Facial geometry + voice print + behavioral biometrics simultaneously	Multiple flagged apps removed from Play Store 2024-2025
Baby/child monitoring	Watch your baby	Continuous facial tracking; emotion detection; sleep state analysis	Child facial biometrics — COPPA implications; may	Various smart baby monitor apps

			create child face database	
Emotion AI analytics	Employee productivity	Continuous webcam monitoring; attention detection; emotion scoring	Employee facial expressions, attention levels, emotional state — workplace surveillance	HireVue, Affectiva, various HR AI platforms

WARNING: BIOMETRIC DATA IS PERMANENT: Unlike passwords, you cannot change your face. Once your facial geometry (a set of mathematical measurements) has been extracted and stored, it can be used to identify you forever — even if the original app is deleted. Facial geometry hashes are highly resistant to disguise and are increasingly used for cross-platform identity correlation without your consent.

2.4 Retail AI Vision — Physical Stores Tracking You

Computer vision is increasingly deployed in physical retail spaces using smartphone apps as the data bridge:

- Store cameras run real-time facial recognition to identify repeat visitors, link in-store behavior to online profiles.
- Retail analytics platforms (Centific Pitaya.AI, Standard Cognition) turn existing CCTV into AI-powered behavioral analysis systems.
- Shopkick-style loyalty apps cross-reference your in-store location (via ultrasonic beacons) with your online purchase history and social media profile.
- Edge AI cameras process and transmit facial geometry to central servers without storing raw video, technically complying with privacy laws while still building facial databases.

3. ADTECH FIRMS WITHOUT RULES — RTB DATA PIPELINE ARCHITECTURE

3.1 What Is Real-Time Bidding (RTB)?

Real-time bidding (RTB) is the automated auction system that underlies modern digital advertising. When you open an app or visit a website, an auction for your attention takes place in under 100 milliseconds. But the auction is not just for your attention — it is for your personal data profile. The ICCL (Irish Council for Civil Liberties) calls it 'the biggest data breach ever recorded.'

Scale: RTB broadcasts personal data 294 billion times per day in the USA and 197 billion times per day in Europe (ICCL, 2022). Google's RTB system alone operates on 33.7 million websites, 92% of Android apps, and 77% of iOS apps (Brave complaint, 2018).

3.2 Complete RTB Data Pipeline Architecture

Step	Component	Technical Role	Data Transmitted	Privacy Problem
1	User opens app or website	An ad slot becomes available	App sends user context to SSP via SDK call	Triggered without user awareness or active consent
2	Supply-Side Platform (SSP)	Publisher's ad revenue system	Packages user data: device ID, location, browsing context, interests, demographics into a 'bid request'	SSP transmits to hundreds of parties simultaneously — IAB confirmed this cannot be disclosed in advance
3	OpenRTB Bid Request	Standardised JSON payload (IAB spec)	Contains: device ID, IP, GPS, user agent, publisher ID, page URL, user interests (595 possible fields), special category data	595 data fields include: Heart Disease, Mental Health, Sexual Health, Reproductive Health, Substance Abuse, Politics, Ethnic Groups — all transmitted in bid requests
4	Ad Exchange	Auction intermediary	Broadcasts bid request to 2,000+ Demand-Side Platforms within 100ms	No technical controls exist to restrict what DSPs do with received data — confirmed by IAB document
5	Demand-Side Platform (DSP)	Advertiser bidding system	Each DSP receives full bid request, evaluates user profile, submits bid or passes	Each of 2,000+ DSPs now holds a copy of your data — with no deletion mandate
6	Data Management	Profile enrichment layer	DSPs cross-reference received data with third-party	Your RTB-derived profile merged with credit data,

	Platform (DMP)		data brokers to enrich user profile	location history, purchase records, offline behavior
7	Data Broker Layer	Profile aggregation and resale	RTB data intercepted and sold by data brokers who are not officially part of the bidding chain	RTB data used to: profile BLM protestors (per ICCL), track military personnel, out a gay priest via Grindr data
8	Winning bid	Ad displayed	Winner serves ad; all other DSPs retain user data from the bid request	Every losing bidder keeps your data permanently — they paid nothing for it

3.3 Why RTB Is Structurally Impossible to Regulate

- Structural impossibility of consent: The IAB's own CEO acknowledged in a 2017 email (obtained via FOIA): 'As it is technically impossible for the user to have prior information about every data controller involved in a real-time bidding scenario, [RTB] would seem, at least prima facie, to be incompatible with consent under GDPR.'
- No technical controls: An IAB Tech Lab document ('pubvendors.json v1.0') explicitly states there are 'no technical measures' to control what companies do with data once it is broadcast in a bid request.
- GDPR has failed: The EU's GDPR has been in force since 2018. Complaints were filed in 2018 and 2019. As of 2025, no substantive enforcement action has stopped RTB. Ireland's DPC (Google's lead regulator) repeatedly failed to act.
- IAB's TCF consent framework failed: Belgium's data protection authority ruled in February 2022 that the IAB Europe's Transparency and Consent Framework (TCF) itself breaches GDPR. The IAB was fined and given six months to reform — the system continues operating.
- Special category data leaks: RTB bid requests routinely include inferred sensitive data: medical conditions, political affiliation, sexual orientation, ethnicity. These categories are supposed to receive heightened protection under GDPR.
- US military exposure: A 2023 Enforce report found that RTB data including data from active US military personnel, national security leaders, and judges was available for purchase on the commercial data market. Companies with 'Beijing' in their title appear on Google's certified RTB partner list.

3.4 Key AdTech Firms and Their Regulatory Status

Company	Role	China / Sensitive Connections	Regulatory Status 2017-2026
Google (Authorized Buyers)	Largest RTB exchange operator; sets Authorized Buyers spec	Certified partners include companies with Beijing in title; RTB transmits to 2,833 companies	FTC investigation 2024; Irish DPC probe ongoing; ICCL lawsuit Germany 2021

IAB / IAB Tech Lab	Sets OpenRTB standard; operates TCF consent framework	Global membership includes Chinese advertising companies	TCF ruled GDPR-violating Feb 2022; IAB fined; reform imposed but system continues
The Trade Desk	Major DSP; AI-powered bidding	Operates in China via TTD China JV; access to Chinese user data flows	No major regulatory action; self-regulated via IAB TCF
Mintegral (Mobvista)	Chinese adtech; SDK embedded in 1,700+ iOS apps	Shenzhen-based; caught clickjacking and intercepting ALL app network requests (not just ads) in 2020	Removed from some app stores temporarily; continues operating
Umeng Analytics (Alibaba)	Alibaba's analytics SDK	Data flows to Alibaba servers in China	Included in thousands of Chinese-origin apps; limited Western regulatory scrutiny
Igexin SDK	Chinese ad SDK	Beijing-based; SDK installed remote code execution capabilities	500+ Google Play apps affected; Lookout research 2017; Google removed affected apps
AppLovin	US mobile adtech	No direct China tie but operates global data harvesting at scale	FTC/state investigations into data practices; acquisitions including MoPub (Twitter)
InMobi	Indian mobile adtech	Operates in China; FTC fined $950,000 in 2016 for tracking children	FTC action 2016; continues global operation

WARNING: AI IN RTB (2023-2026): Adtech firms have integrated AI models into bidding systems that can infer sensitive attributes (health conditions, pregnancy, sexual orientation, political views) from behavioral signals alone — even without explicit data in the bid request. These AI-inferred profiles are being bought and sold without any regulatory framework governing AI inference in advertising.

4. AI MODEL TRAINING ON YOUR DATA — THE SUBSCRIPTION LOOP

4.1 The Complete Pipeline: Free App → AI Training → Paid Product

The most sophisticated exploitation of user data follows a five-stage cycle: (1) offer a free service that collects data, (2) use that data to train AI models, (3) productise the AI model, (4) sell access as a subscription, (5) use subscription revenue to collect more data. The user is both the raw material and the eventual customer.

Stage	What Happens	Your Data's Role	Product Created
1: Free app	User downloads free AI chat, beauty filter, voice assistant, or dating app	App collects: voice audio, photos, behavioral data, social graph, location history	Data asset — raw training material
2: Data annotation	Collected data is labelled, cleaned, and structured for training	Your voice recordings are transcribed and tagged; your facial photos are annotated with attributes	Supervised training dataset worth millions of dollars
3: Model training	Data used to train neural networks (speech recognition, facial recognition, LLM, recommendation engine)	Your data improves model accuracy — you are effectively unpaid labour for the training run	Trained AI model — proprietary asset
4: Model deployment	Trained model is deployed as API or embedded product	Your data's contribution is now baked into the model's weights permanently	Commercial AI product
5: Subscription sale	Product sold as subscription: voice cloning API, facial recognition API, AI assistant, personalised recommendation engine	You may even pay to access a product trained on your own data	Revenue stream — model sold back to users and enterprises

4.2 Voice Data — Training and Commercial Exploitation

Capability	Technical Requirement	How Apps Collect It	Commercial Product
Voice cloning	3–10 seconds of clean audio	Voice assistant apps, audiobook apps, social audio apps collect samples during normal use	ElevenLabs, Respeecher, Microsoft VALL-E — voice synthesis APIs

Speech recognition	Hours of labelled speech	Voice search, dictation, and transcription apps collect all audio with text ground truth	Google, Apple, Amazon, Baidu speech recognition APIs
Speaker identification	Multiple voice samples per person	Smart speaker apps, customer service bots, video call platforms capture speaker profiles	Voiceprint authentication systems sold to banks and call centres
Emotion detection from voice	Labelled emotional speech samples	Customer service apps, mental health apps, social media voice features	Entropik, Cogito, Behavioral Signals — emotion AI for call centres
Accent and language classification	Diverse speech samples	Translation apps, language learning platforms, global voice assistants	Demographic targeting by language region and accent

4.3 AI Models Without Oversight — The Regulatory Gap

As of 2026, there is no comprehensive global regulatory framework specifically governing:

- How AI models trained on user data must disclose their training sources
- Whether users have rights to deletion from AI model weights (GDPR's right to erasure is practically impossible to implement in trained neural networks)
- Whether AI models can be sold across borders if trained on data from restricted jurisdictions
- How AI-inferred attributes (health status, sexuality, political views) in adtech are regulated differently from explicitly collected attributes
- What constitutes adequate consent for biometric AI training

The EU AI Act (fully in force 2026) classifies some uses as 'high risk' but creates exemptions for advertising and commercial profiling. The US has no comprehensive federal AI regulation. China's AI regulations apply to domestic use but not to data exported and processed overseas.

5. ANDROID PERMISSION EVOLUTION — YEAR BY YEAR (2015–2026)

5.1 The Permission System Architecture

Android's permission system has been redesigned multiple times since Android 1.0 (2008). The most significant architectural shift came with Android 6.0 Marshmallow (2015), which introduced runtime permission requests — replacing the install-time 'accept all or don't install' model. Each subsequent Android version has tightened specific permissions while threat actors continually adapted.

Android Version	Year Released	Key Permission Changes	What It Closed / What Remained Open
Android 1.0–5.1	2008–2015	Install-time permissions only. User must accept ALL permissions listed in manifest before installing. No granularity.	CLOSED: Nothing — all permissions granted at install. OPEN: Everything — full access to all declared permissions with no per-use prompt.
Android 6.0 Marshmallow	October 2015	RUNTIME PERMISSIONS introduced. 'Dangerous' permissions now require in-app popup approval. Users can deny individual permissions. Revocation via Settings > Apps.	CLOSED: Silent batch permission grants. OPEN: Apps could still request permissions and re-ask repeatedly. No background restriction. 'Normal' permissions still auto-granted.
Android 7.0-7.1 Nougat	August 2016	Doze Mode enhanced — restricts background processing for battery but helps privacy. Apps restricted from using implicit intents for certain broadcasts.	CLOSED: Some broadcast receivers auto-triggered on boot. OPEN: Background location still available; no limits on how often apps could access microphone/camera.
Android 8.0-8.1 Oreo	August 2017	Background execution limits — apps can no longer run persistent background services without foreground notification. Introduced READ_PHONE_NUMBERS permission split from READ_PHONE_STATE.	CLOSED: Silent background services harvesting data. OPEN: Foreground services (with visible notification) still allow continuous background operation. INSTALL_PACKAGES from unknown sources per-app.
Android 9.0 Pie	August 2018	Apps in background CANNOT access camera or microphone. Inactive apps removed from recently used mic/camera. Wi-Fi scanning requires location permission.	CLOSED: Background camera/mic access by non-foreground apps. OPEN: Foreground apps with notification can still record continuously. No limit on location polling frequency.
Android 10	September 2019	Background location requires explicit ACCESS_BACKGROUND_LOCATION permission (separate from foreground). Scoped Storage introduced — apps can no longer access all files. MAC address randomisation per network. READ_CLIPBOARD access restricted.	CLOSED: Silent background GPS tracking (must now show clear notification or get separate permission). OPEN: Apps could still request background location; many users grant it. Clipboard

			access still possible within foreground.
Android 11	September 2020	One-time permissions for mic, camera, location. Auto-reset permissions for unused apps. Background location now requires separate Google approval for Play Store apps. Scoped Storage enforcement.	CLOSED: Persistent permissions for rarely used apps (auto-reset). OPEN: One-time permissions can be re-requested. Accessibility services still have very broad access. READ_PHONE_STATE still reveals IMEI on older APIs.
Android 12	October 2021	Approximate location option (user can grant approximate instead of precise). Privacy dashboard showing which apps used camera, mic, location in past 24h. Microphone and camera indicators (green dot in status bar). Clipboard read auto-notified to user.	CLOSED: Silent precise GPS tracking — users now see the indicator. OPEN: Approximate location still useful for targeting. Camera/mic indicator can be dismissed. No restriction on total number of permission requests.
Android 13	August 2022	Granular media permissions: READ_MEDIA_IMAGES, READ_MEDIA_VIDEO, READ_MEDIA_AUDIO replace READ_EXTERNAL_STORAGE. Notification permission now runtime. Photo picker (user selects specific photos; app cannot see all photos). Nearby Wi-Fi permission split from location.	CLOSED: Apps reading all photos/files via storage permission. OPEN: Apps that already have permissions retain them. Notification permission — users often click Allow out of habit.
Android 14	October 2023	Partial photos access (user selects specific media items). USE_FULL_SCREEN_INTENT restricted to calling/alarm apps only. Health Connect permissions more granular. Data safety info shown in permission dialogs.	CLOSED: Full photo library access (apps now see only selected photos). OPEN: Accessibility services still very broad — used by SpyNote/SpyMax malware extensively in 2024-2025. Dynamic code loading still possible (exploited by malware).
Android 15	September 2024	Theft protection: locks screen if sudden acceleration detected (phone snatching). Private Space feature — apps in private space hidden from others. Health data protections enhanced. Satellite connectivity permissions. Content:// URI is now standard for all file access.	CLOSED: Some theft scenarios; enhanced private area. OPEN: BIND_ACCESSIBILITY_SERVICE still grants near-total device control. Background app permission abuse via updates (versioning attack) still possible. AI-powered inference of sensitive attributes from permitted data not restricted.
Android 16 (Preview)	Expected 2025–2026	Enhanced scam call protection. AI-powered permission anomaly detection. Further restrictions on background process communication.	TBD — no final specification released as of April 2026

6. HOW MALICIOUS APPS BYPASS ANDROID PERMISSIONS

6.1 Permission Bypass Techniques Used by Malware (2017–2026)

Even as Android has tightened permissions year by year, sophisticated malware and adtech have developed techniques to access sensitive data without the expected permissions — or to obtain permissions through deception.

Bypass Technique	Technical Method	Permissions Needed	What It Harvests	Us
BIND_ACCESSIBILITY_SERVICE abuse	Registers as accessibility tool; gains ability to read screen content, click UI elements, monitor all input	BIND_ACCESSIBILITY_SERVICE (user must grant in Settings)	Passwords typed on screen, banking OTPs, all text on screen, app content, keystrokes — functionally a full keylogger	Sp (20 ba Ma (20
Versioning / Update injection	App passes Play Store review as clean; malicious payload delivered via app update days/weeks later	Whatever the original app declared	Anything the app's declared permissions allow — but now with malicious intent hidden inside a trusted update	33 ca 202 ad ca (20
Dropper / downloader	App uses INSTALL_PACKAGES to silently install secondary APK containing full malware payload	INSTALL_PACKAGES (or user enabled Unknown Sources)	Secondary APK can request additional permissions; the dropper app appears clean	Ige (20 Ca (20 ba
Accessibility-to-clipboard	Accessibility service reads clipboard content on each change — bypasses Android 10+ clipboard restrictions for foreground apps	BIND_ACCESSIBILITY_SERVICE	Passwords copied to clipboard, crypto wallet addresses, OTPs, all clipboard content	Ba (20
Screen capture via MediaProjection	Requests MEDIA_PROJECTION permission via system	MEDIA_PROJECTION (runtime dialog)	Everything visible on screen —	Re troj 202

	dialog; screenshots or screen recordings taken continuously		banking apps, email, photos, private messages	
Microphone via background workaround	Uses a foreground service with visible notification to maintain mic access; notification designed to look like legitimate system notification	RECORD_AUDIO + foreground service	Continuous audio recording despite Android 9+ background mic restrictions; notification can be made nearly invisible	Sp ca tar (Ba MC 202
Side-channel: accelerometer audio	Accelerometer data (no permission required) can reconstruct speech at close range — demonstrated by academic researchers	NONE — accelerometer requires no permission	Partial speech reconstruction from device vibration when placed near a speaker	Re de no wi ma
INSTALL_PACKAGES via WebView	App displays web content that prompts installation; uses Android's custom URL scheme to trigger APK download from app's own assets	REQUEST_INSTALL_PACKAGES	Bypasses Play Protect for the secondary payload if it appears to come from user interaction	Ma ca fak ap 202
Wi-Fi probe requests	Passive Wi-Fi probe monitoring without any permission captures nearby device identifiers; Android 9 randomised MAC but nearby AP SSIDs still reveal location patterns	None (passive listening)	Location inference from known Wi-Fi networks; device presence tracking in physical spaces	Re SD res 202

6.2 Permissions That Cannot Be Denied — Special Access

Certain Android permissions cannot be granted through the normal runtime permission dialog. They require users to navigate to specific Settings pages — and malware is designed to guide users through this process using social engineering.

Special Permission	How to Grant	Why Malware Wants It	Abuse Level
BIND_ACCESSIBILITY_SERVICE	Settings > Accessibility > [App Name] > Enable	Full screen reading, input injection, app monitoring — effectively total device control	CRITICAL — Used by nearly all advanced Android spyware
BIND_DEVICE_ADMIN	Settings > Security > Device Administrators > [App Name]	Cannot be uninstalled while active; can remotely wipe device; can enforce screen lock	CRITICAL — Ransomware and stalkerware use this for persistence
SYSTEM_ALERT_WINDOW	Settings > Apps > [App Name] > Display over other apps	Draw overlays over other apps — used for banking credential phishing overlays	HIGH — Used by banking trojans to overlay fake login screens on legitimate banking apps
WRITE_SETTINGS	Settings > Apps > Special app access > Modify system settings	Change system settings: screen brightness, volume, WiFi, Bluetooth, etc.	HIGH — Can disable security features, enable unknown sources programmatically
MANAGE_EXTERNAL_STORAGE	Settings > Apps > [App Name] > Files and media > Allow management of all files	Access ALL files on device regardless of Scoped Storage (Android 11+ bypass)	HIGH — Circumvents Android 11+ Scoped Storage protections
REQUEST_INSTALL_PACKAGES	Settings > Apps > [App Name] > Install unknown apps	Install additional APKs silently or via deceptive prompts	HIGH — Primary mechanism for dropper malware second-stage delivery
NOTIFICATION_LISTENER	Settings > Notifications > Notification access > [App Name]	Read ALL notifications from ALL apps — including 2FA codes, banking alerts, messages	CRITICAL — 2FA theft without needing SMS permission on Android 12+

7. HOW DATA REACHES CHINA WITHOUT YOUR KNOWLEDGE

7.1 Legal Framework Enabling Forced Data Access

Chinese Law	Year Enacted	Key Provision	Effect on Apps
National Intelligence Law	2017	Article 7: 'Any organization or citizen shall support, assist and cooperate with the state intelligence work in accordance with the law'	ALL Chinese companies and citizens MUST provide data to Chinese intelligence on demand — regardless of where the company is registered or where data is stored
Cybersecurity Law	2017	Requires 'critical information infrastructure operators' to store data within China; mandates security reviews	Chinese apps must have the ability to transmit data to Chinese servers; any 'security review' effectively grants access
Data Security Law	2021	Regulates data processing; restricts transfer of 'important data' abroad; broad definition of important data	Creates data residency requirements; mandates government access to data classified as important
Personal Information Protection Law (PIPL)	2021	China's version of GDPR — but with mandatory government access exemptions	While providing user rights similar to GDPR, exempts government/intelligence access — fundamentally different from Western privacy laws
Regulations on Internet Information Services	Ongoing revisions	Content control; user identity registration; real-name requirements	All Chinese apps must maintain user identity data accessible to regulators

7.2 The Singapore Shell Architecture

Singapore became the preferred routing point for Chinese tech companies' international data operations because:

- Singapore is not subject to Chinese data localisation laws on its face — data stored in Singapore appears legally separate from Chinese jurisdiction.
- Singapore has a trusted international reputation and strong commercial law — reducing scrutiny from Western partners.
- Singapore's PDPA (Personal Data Protection Act) is less restrictive than GDPR — less enforcement risk.
- Physical proximity to Chinese data centres means low-latency mirroring is technically straightforward.
- Singapore-registered companies can open US App Store and Google Play developer accounts without triggering national security reviews that a PRC-registered company might.

Despite the legal separation, the National Intelligence Law's reach extends to any Chinese citizen or organization anywhere in the world — meaning a Singapore-registered subsidiary of a Chinese parent company is still subject to Chinese intelligence demands through the parent company relationship.

7.3 TikTok Singapore Architecture — Documented Case Study

Element	Detail	Source
Singapore legal entity	TikTok Ltd., Singapore — subsidiary of ByteDance, Beijing	Corporate filings
Poligon Pte. Ltd.	Singapore ByteDance subsidiary operating Melolo and Fizzo apps in Southeast Asia — pulled from US stores January 2025	PAFACA enforcement; Newsweek 2025
Stated data storage	TikTok claimed US user data stored in Oracle servers (Project Texas) with Singapore backup	TikTok congressional testimony 2022
Actual access	Leaked audio from 80 internal meetings: China-based ByteDance employees accessed non-public US user data; 'master admin' could see everything	BuzzFeed News, June 2022
Employee instruction	A data scientist in a January 2022 meeting stated: 'I get my instructions from the main office in Beijing'	BuzzFeed News, leaked audio
Project Texas reality	CFIUS negotiations confirmed that even under Project Texas, UIDs (device identifiers) were NOT classified as protected data — accessible from China	BuzzFeed News leaked audio; Senate Intel Committee
Biometric collection	TikTok's privacy policy updated June 2021 to include potential collection of 'faceprints and voiceprints'	TikTok Privacy Policy
FTC action	FTC + DOJ filed joint lawsuit August 2024 alleging violations of 2019 COPPA consent decree — children's data improperly collected	FTC/DOJ court filings
US ban	Supreme Court upheld PAFACA unanimously; TikTok, CapCut, Lemon8, TikTok Studio, Melolo, Fizzo removed from US app stores January 19, 2025	US Supreme Court ruling

8. TIMELINE OF KEY ARCHITECTURE CHANGES 2017–2026

Year	Audio Beacon	AI Vision	AdTech RTB	Android Permissions	China / Regulation
2017	234 apps found with Silverpush SDK; Google removes them; FTC warnings issued; Silverpush pivots away from beacons	Face++ (Megvii) widely available; beauty app explosion; 106-point facial mapping in millions of apps	IAB employee acknowledges RTB incompatible with GDPR (internal email); GDPR not yet in force	Android 8.0: Background execution limits; service restrictions	India IB flags 42 Chinese apps as spyware; Chinese National Intelligence Law enacted; UC Browser DNS hijacking case
2018	LISNR pivots to contactless payments; uXDT technology fades from apps but enters infrastructure	BeautyPlus (Meitu) caught collecting IMEI, carrier, WiFi data; sent to Chinese servers	GDPR in force May 25; Brave files first RTB complaints; Google/IAB deny problems	Android 9: Camera/mic blocked for background apps — major security improvement	GDPR takes effect; Cheetah Mobile implicated in click fraud (Kochava); 7 Cheetah apps investigated
2019	Signal360/Shopkick largely retired from ad tracking; ultrasonic tech moves to retail analytics	ARKit and ML Kit facial tracking reach millions of apps; Clearview AI begins scraping	IAB TCF v1.0 launches — later ruled GDPR-violating; FTC fines InMobi $950K for children tracking	Android 10: Background location separated; Scoped Storage; MAC address randomisation	ES File Explorer removed from Play; CamScanner Trojan found; India flags more Chinese apps
2020	Ultrasonic payments (LISNR/Mastercard) go commercial; retail tracking via audio continues invisibly	Mintegral SDK caught intercepting ALL iOS app network requests (not just ads) — 1,700+ iOS apps affected	ICCL report: RTB broadcasts data 294B times/day in USA; ICO warns RTB 'out of control'	Android 11: One-time permissions; auto-reset unused permissions; background location needs Play approval	India bans 59 Chinese apps June 29 (TikTok, UC Browser, WeChat, Clean Master, SHAREit, 55 others); Cheetah Mobile: Google bans all 45 apps Feb 2020
2021	Acoustic attack research: accelerometer data can	Clearview AI fined in multiple countries; facial recognition market reaches	Belgian DPA: TCF framework breaches GDPR; ICCL	Android 12: Green dot camera/mic indicator; privacy dashboard; approximate location	UC Browser caught sending IP to Alibaba servers; APKPure infected

	reconstruct speech — no permission needed	$3.86B; TikTok updates privacy policy to include faceprints/voiceprints	takes IAB to German court	option; clipboard notification	with malware April 2021; China PIPL and Data Security Law enacted
2022	LISNR used in contactless payment terminals globally; few consumer apps still use direct audio beacons	EU AI Act negotiations include facial recognition restrictions; Clearview AI banned EU/UK; Face++ continues operating globally	BuzzFeed 80-meeting leak: TikTok/ByteDance China access confirmed; IAB TCF ruled GDPR-violating Feb 2022	Android 13: Granular media permissions; photo picker; notification permission runtime; Wi-Fi nearby split from location	BuzzFeed leaks TikTok audio; India bans 54 more Chinese apps; FTC opens TikTok investigation; CFIUS negotiations stall
2023	SilverPush 'Mirrors' AI video ad platform grows — analyzes video content user watches; no audio beacons needed	Emotion AI embedded in HR platforms (HireVue); deepfake apps proliferate on Play Store; Google Play hosts deepfake generators	RTB AI profiling: DSPs infer health, sexuality, politics from behavioral signals without explicit data in bid request	Android 14 (Oct 2023): Partial photos access; USE_FULL_SCREEN_INTENT restricted; Health Connect permissions	331 apps with 60M downloads running ad fraud; FTC active TikTok investigation; India total Chinese app bans exceeds 400
2024	NFC relay attacks become dominant attack vector — replaces some audio attack scenarios	MOONSHINE/BadBazaar spyware targets Uyghur/Tibetan communities via fake apps with camera/mic access	Complaint: Google's RTB system shares data with companies with 'Beijing' in title; military personnel data available commercially	Android 15 (Sept 2024): Theft protection; Private Space; satellite permissions; content URI standard	FTC+DOJ joint lawsuit vs TikTok/ByteDance Aug 2024; SpyNote/Gigabud attributed to Chinese GoldFactory group; MOONSHINE/BadBazaar joint Five Eyes advisory
2025-2026	Ultrasonic tech integrated into smart home, IoT, payment infrastructure — harder to detect, less visible	EU AI Act fully in force; facial recognition 'high risk' classification; emotion recognition restricted in workplaces	By 2026: 90% of global display ad budget flows through programmatic/RTB; AI bidding systems dominate; no effective regulation	Android 16 preview: AI permission anomaly detection; enhanced scam call protection	US Supreme Court: TikTok banned Jan 2025; partially restored; Google Play blocks 1.75M apps in 2025; Kaspersky: Android attacks up 50% in 2025

9. REGULATORY FAILURES AND WHAT ACTUALLY WORKS

9.1 What Has Failed

- GDPR (EU, 2018): RTB still operates with 294 billion daily broadcasts. IAB TCF framework ruled GDPR-violating in 2022 — system still running. No major adtech company shut down for GDPR violations.
- CCPA (California, 2020): Data brokers still operate; opt-out mechanisms technically available but impractical at scale; no audit of compliance.
- FTC enforcement: InMobi fined $950K (2016) — trivial relative to revenues. TikTok/ByteDance lawsuit filed 2024 — outcome pending. Silverpush: warning letters only, no fines.
- Google Play self-policing: 234 ultrasonic apps removed (2017), 600 Cheetah apps removed (2020), 2.36M apps blocked (2024) — but the system is reactive, not preventive. Versioning bypasses initial review.
- App store transparency reports: Data safety section on Google Play is self-declared by developers — no verification. Multiple cases of apps lying about data collection.

9.2 What Has Actually Worked

- Government bans with enforcement: India's ban of 400+ Chinese apps effectively removed them from Indian devices. US PAFACA enforcement removed TikTok from US app stores. More decisive than any regulatory fine.
- Platform-level technical controls: Android 9 background camera/mic restriction genuinely reduced background surveillance. Android 10 background location separation was effective. Android 13 granular media permissions meaningfully reduced photo access.
- Security research pressure: Citizen Lab, Braunschweig researchers, and Lookout publications forced Google to remove specific apps and SDKs faster than any regulatory action. Academic research on ultrasonic beacons led to Play Store enforcement within months.
- Google Play Protect: Real-time scanning of 200 billion apps daily provides a genuine technical barrier. Play Protect identified 13 million new malware threats outside Play Store in 2024.
- Private Space (Android 15): Technically effective isolation of sensitive apps from app surveillance.

9.3 User-Level Protections That Work

- Deny RECORD_AUDIO to any app that does not need it for a clear stated purpose (voice calls, music recording). The RECORD_AUDIO permission is the gate for all audio beacon harvesting.
- Deny CAMERA to apps that do not obviously need it. A shopping app, finance app, or news app has no legitimate need for camera access.
- NEVER grant BIND_ACCESSIBILITY_SERVICE to any app that is not a legitimate accessibility tool (screen reader, switch control). This is the master key that gives apps near-total device control.

- Check the Privacy Dashboard (Android 12+): Settings > Privacy > Privacy Dashboard — see exactly which apps accessed mic, camera, and location in the past 24 hours. Revoke anything suspicious.
- Use the one-time permission option whenever available. Apps that need mic access for a single voice search do not need persistent permission.
- Install SoniControl (open source Android app) to detect and block ultrasonic beacon frequencies in your environment.
- Use a VPN — but research the provider carefully. Many free VPN apps are themselves data harvesting tools. Malwarebytes September 2025 found popular Android VPN apps with undisclosed China links.
- Assume APKPure is unsafe. Every app on APKPure should be treated as potentially modified. The platform itself was compromised by Trojan malware in April 2021.

— END OF ARCHITECTURE REPORT —

Sources: Citizen Lab, Braunschweig TU, ICCL, Brave, ICO, FTC, Kaspersky, Zimperium, Lookout, BuzzFeed News, EFF | April 2026