# CLASSIFIED INVESTIGATION DOSSIER

**SUBJECT:**

## SILVERPUSH (SilverEdge Technologies Pvt. Ltd.) & InMobi Pte. Ltd.

*Adtech Digital Surveillance Operations: Modus Operandi, Privacy Violations, Regulatory Failures & Investigative Framework for Prosecution*

| | |
|---|---|
| **Prepared For** | Investigating Officer — Cybercrime / Digital Forensics Unit |
| **Classification** | **SENSITIVE — Law Enforcement Only** |
| **Date Compiled** | March 2026 |

# SECTION 1: COMPLETE IDENTITY PROFILE — SILVERPUSH

## 1.1 Legal Entity & Corporate Names

| | |
|---|---|
| **Full Legal Name (India)** | Silveredge Technologies Private Limited |
| **Brand / Operating Name** | SilverPush |
| **CIN (MCA India)** | U72900DL2012PTC242716 |
| **Legal Entity Identifier** | 984500C56C670FBD0484 |
| **Incorporated** | 25 September 2012 (India) \| September 2012 (Singapore entity) |
| **Company Type** | Private Limited Company — Non-Government |
| **Registered Under** | Registrar of Companies (RoC), Delhi |
| **Singapore Entity** | Silverpush Pte. Ltd. (Singapore-based marketing tech provider) |
| **Industry Code (NIC)** | 7290 — Other Computer Related Activities |
| **Authorized Share Capital** | INR 3,19,00,000 |
| **Paid-Up Capital** | INR 1,48,81,000 |
| **Revenue (FY2024)** | INR 345 Crore (approx USD 41M) |
| **Employees (Mar 2024)** | 88 (India entity) |
| **Status (MCA)** | ACTIVE |
| **Last AGM** | 23 December 2023 |
| **Balance Sheet Filed** | 31 March 2023 |
| **Countries of Operation** | 11+ countries including India, Singapore, USA, Vietnam, Philippines, Malaysia, UAE, Indonesia |

## 1.2 Registered & Operational Addresses

| | |
|---|---|
| **Registered Office (MCA)** | T-19 Basement, Green Park Main, New Delhi, Delhi — 110016, India |
| **Email (MCA)** | accounts@silverpush.co |
| **HQ (Operational)** | Grand View Tower, 17th Floor, Golf Course Extension Road, Sector 58, Badshahpur, Gurgaon, Haryana — 122101, India |
| **Older Gurgaon Office** | 3rd Floor, Unit No. C 349-354, JMD Megapolis, Sohna Road, Sector 48, Gurgaon, Haryana — 122018 |
| **Singapore HQ** | Singapore (primary global HQ per company claims) |

| | |
|---|---|
| **Origin City** | Gurugram (Gurgaon), Haryana, near New Delhi — CONFIRMED by FTC and CDT documents |

*INVESTIGATOR NOTE: A gap exists between the legal registered address (Green Park, Delhi) and the operational HQ (Gurgaon). This is a common structural pattern used by Indian tech startups to exploit lower compliance visibility. The Singapore registration creates an additional jurisdictional layer that complicates Indian enforcement.*

## 1.3 Directors & Key Personnel

| | |
|---|---|
| **Founder & CEO** | Hitesh Chawla — IIT Delhi (B.Tech 1999–2004), Research Associate at Univ. of Michigan (2002), Research Scientist at Univ. of New South Wales (2004–2005), Analyst at Evalueserve (2005–2008) |
| **Co-Founder (CMO)** | Mudit Seth — IIM Ahmedabad graduate; previously AdGlobal360, Wildnet Technologies, Tyroo Media; co-founded Wiseassist Technologies with Chawla |
| **Co-Founder (US)** | Alex Modon (also listed as Alex Moon) — BS in e-marketing, advertising, Univ. of Akron Honors College, USA; previously Face to Face Tutoring |
| **Director** | Sneha Khemani |
| **Director** | Vidur Vishnu Bhogilal — Appointed 09 March 2023 |
| **Director** | Siddharth Pradip Kothari — Appointed 05 November 2022 (also Managing Director at JM Financial Private Equity — KEY INVESTOR) |
| **Company Secretary** | Chandra Kishor Jha — Appointed 06 August 2022 |
| **Previous Role — Chawla** | Co-founder, Wiseassist Technologies (sold before SilverPush); product: 'Wisetouch' (ad platform for outdoor media) |

## 1.4 Funding & Investors

| | |
|---|---|
| **Series A (April 2014)** | USD 1.5 million — for global expansion |
| **Investors (Early)** | IDG Ventures, Palaash Ventures, Fabrice Grinda (angel), K. Ganesh, 500 Startups, M&S Partners |
| **Series B (February 2019)** | USD 5 million — FreakOut Holdings (Japan) / Freak Out Inc., Japan |
| **Series C (November 2022)** | USD ~12 million (INR 950 million) led by JM Financial Private Equity, with Ashish Kacholia, Mirabilis Investment Trust, Seven Hills Capital |
| **Founder Net Worth** | INR 103 Crore (as of July 2023) |
| **Ownership** | Founders: 19.98% \| Funds: 14.38% \| Angels: 4.31% \| Parent Entities (largest): 48.42% |

## 1.5 GST Registration Status

| | |
|---|---|
| **Total GST Registrations** | 5 GST numbers across 5 states |
| **GST — Delhi** | 07AASCS2257G1Z1 — INACTIVE |
| **GST — Haryana** | 06AASCS2257G1Z3 — ACTIVE |
| **Other States** | 3 additional registrations (status: inactive) |
| **INVESTIGATOR FLAG** | Inactive GST in Delhi despite having registered office in Delhi raises MCA compliance gap. Company appears to have moved operations to Haryana (Gurgaon) while retaining legal address in Delhi — requires examination for tax compliance issues. |

# SECTION 2: MODUS OPERANDI — DIGITAL SURVEILLANCE TECHNOLOGY

## 2.1 Core Technology: Ultrasonic Audio Beacons (uXDT)

SilverPush developed a proprietary 'Unique Audio Beacon' technology — a form of Ultrasonic Cross-Device Tracking (uXDT) — that operates at frequencies between 18kHz and 19.95kHz. These frequencies are above the threshold of human hearing but detectable by device microphones.

### How It Works — Step by Step:

- Step 1: SilverPush embeds inaudible high-frequency tones into TV advertisements and web browser ads. Each tone carries encoded data (e.g., letter 'A' = 18kHz tone, 'P' = 19.125kHz — enabling ad identification such as a Geico commercial = 'AP').
- Step 2: Mobile apps integrated with the SilverPush SDK silently activate the device microphone — even when the app is NOT in active use (background listening).
- Step 3: The microphone continuously scans for these beacon frequencies. Upon detection, a 'pair' is made between the user's device and the TV/screen content being viewed.
- Step 4: The individual device ID is mapped to the user's 'audience genome' — a behavioral profile built from TV viewing habits, location, and cross-device activity.
- Step 5: The collected data is transmitted to SilverPush's remote servers, building detailed logs of television content viewed, advertising exposure, and consumer profiling.
- Step 6: Advertisers use this data for hyper-targeted advertising, cross-device campaign synchronization, and behavioral analytics.

**CRITICAL FINDING — FTC Confirmed**
The software activates the device microphone even when users have not granted microphone permission to the app, and even when users are not actively using the application. No disclosure was given to users. This constitutes covert surveillance.

## 2.2 Product Portfolio Timeline

| | |
|---|---|
| **2012** | Founded as SilverEdge Technologies; initial push notification advertising platform |
| **2013** | Launched push notification advertisement service |
| **2014** | Launched India's first DSP (Demand Side Platform); audio beacon technology deployed |
| **2015** | Claimed 67 apps using its SDK with audio beacons; began TV ad tracking covering 13,000+ ads across 400 channels daily |

| | |
|---|---|
| **2016 (Post-FTC)** | Officially announced ending Unique Audio Beacon service; however continued advertising the service on website as of March 21, 2016 — 4 days after announcement |
| **2017** | 234 Android apps found by TU Braunschweig researchers to STILL use ultrasonic beacons — despite claimed discontinuation. UCL/UCSB/PoliMI research demonstrated beacons can deanonymize Tor users. |
| **2019 (April)** | Launched 'Parallels' — real-time ad-sync with physical events |
| **2019 (Nov)** | Launched 'Mirrors' — AI/computer vision based in-video contextual ad targeting |
| **2020** | Launched 'Mirrors Safe' — brand safety platform |
| **2022** | Raised USD 12M Series C; expanded to Vietnam, Philippines, Malaysia |
| **2024–2025** | Continues global expansion; claims 'privacy-first' positioning while operating cross-device tracking via new AI methodologies |

**MODUS OPERANDI — PATTERN OF DECEPTION**
SilverPush claimed to end audio beacon surveillance in March 2016. Yet: (1) they continued advertising it on their website days later; (2) researchers in 2017 found 234 apps STILL using it. This demonstrates a consistent pattern of making false public statements to regulators while continuing prohibited operations — a key element for fraud and deceptive practices charges.

## 2.3 Data Harvested — Categories

- Television viewing habits (what shows, what ads, what times)
- Precise geolocation data (current location, historical location, 2-month location history)
- Audio environment (via continuous background microphone access)
- WiFi network identifiers (BSSID/SSID — used to infer location even when GPS disabled)
- Cross-device behavioral profiles (linking phone, TV, tablet, computer activity to a single identity)
- Unique device identifiers (IDFA, Android Ad ID, IMEI-derived identifiers)
- Consumer behavioral patterns (purchase intent, ad exposure history)
- Children's data (collected in child-directed apps without parental consent — COPPA violation via affiliated company InMobi)

# SECTION 3: REGULATORY ACTIONS, FINES & WARNINGS

## 3.1 United States — FTC Warning Letters (March 17, 2016)

Issuing Authority: U.S. Federal Trade Commission (FTC), Bureau of Consumer Protection

Issued By: Maneesha Mithal, Associate Director, Division of Privacy and Identity Protection; Jessica Rich, Director, Bureau of Consumer Protection

Reference URL: https://www.ftc.gov/news-events/news/press-releases/2016/03/ftc-issues-warning-letters-app-developers-using-silverpush-code

### Nature of Warning:

- Warning letters sent to 12 Android app developers using SilverPush SDK
- Apps available on Google Play Store contained SilverPush audio beacon functionality with ZERO disclosure to users
- Apps required microphone permission with no evident functionality requiring it
- Software ran silently in background even when app was not in use
- Potential violation of Section 5 of the FTC Act (prohibition on unfair or deceptive acts or practices in commerce)

> **FTC Direct Quote — For Court Record**
> 'These apps were capable of listening in the background and collecting information about consumers without notifying them.' — Jessica Rich, Director, FTC Bureau of Consumer Protection (March 17, 2016)

CRITICAL GAPS: (1) The FTC issued warnings to app DEVELOPERS but NOT directly to SilverPush itself. (2) No fine was imposed on SilverPush. (3) The FTC accepted SilverPush's self-reported claim that beacons were not embedded in US TV programming — but did not verify this independently. (4) The company was given the opportunity to self-regulate, which evidence shows they failed to do.

## 3.2 Prior Investigative Actions — Center for Democracy & Technology (CDT)

In October 2015, CDT submitted formal comments to the FTC regarding SilverPush's cross-device tracking. CDT stated: 'The only factor that hinders the receipt of an audio beacon by a device is distance and there is no way for the user to opt-out of this form of cross-device tracking.'

CDT's chief technologist Joe Hall noted: 'This kind of technology is fundamentally surreptitious in that it doesn't require consent; if it did require it then the number of users would drop.'

EPIC (Electronic Privacy Information Center) separately filed complaints with the FTC that precipitated the 2016 warning letters.

## 3.3 Academic Research Confirming Continued Operation

- November 2016: UCL (University College London), UCSB (Univ. of California Santa Barbara), and Politecnico di Milano researchers demonstrated that SilverPush uXDT technology could DEANONYMIZE Tor users — exposing activists, journalists, and whistleblowers. Published: 'Listening to Your TV: De-anonymizing Ultrasound Cross-Device Tracking'
- May 2017: Researchers from Technical University Braunschweig (Germany) discovered 234 Android apps still employing ultrasonic tracking beacons — AFTER SilverPush's claimed discontinuation. Apps were available on Google Play Store.
- This research constitutes independent verifiable evidence that SilverPush's 2016 public discontinuation announcement was false.

## 3.4 InMobi (Connected Company) — FTC Enforcement Action & Fine (June 2016)

InMobi Pte. Ltd. is a Singapore-based mobile advertising company with Indian origins (founded in Bangalore, India), operating parallel to SilverPush in the same adtech ecosystem.

| | |
|---|---|
| **Case Reference** | FTC v. InMobi Pte. Ltd., N.D. Cal., 2016 |
| **Fine Imposed** | USD 4 million civil penalty (suspended to USD 950,000 based on financial condition) |
| **Violation 1** | Deceptive location tracking of hundreds of millions of consumers including children WITHOUT consent — even when device privacy settings explicitly denied permission |
| **Violation 2** | COPPA (Children's Online Privacy Protection Act) violation — tracked children's geolocation in thousands of child-directed apps without parental consent |
| **Scale** | 1+ billion devices reached; thousands of apps; 6 billion ad requests per day |
| **Method** | Used WiFi BSSID identifiers to triangulate precise location — bypassing iOS and Android location permission systems entirely |
| **Remediation Order** | 20-year independent biennial privacy audits; delete all children's data; delete all unauthorized location data; prohibited from misrepresenting privacy practices |
| **Court** | U.S. District Court, Northern District of California |
| **Filed By** | U.S. Department of Justice on behalf of the FTC |
| **Ref URL** | https://www.ftc.gov/news-events/news/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges |

INVESTIGATOR NOTE: InMobi represents the enforcement template for what SilverPush should have faced. Both companies: (a) are Singapore-registered with India operations; (b) harvested location/behavioral data covertly; (c) operated in thousands of apps simultaneously; (d) claimed compliance while violating it. InMobi was caught because a COPPA hook existed. SilverPush avoided direct FTC enforcement by claiming US-market non-deployment — a claim that was never independently verified.

# SECTION 4: INDIA OPERATIONS & REGULATORY FAILURES

## 4.1 Entry Into India & Scale of Operations

- SilverPush was FOUNDED in India (Gurgaon, Haryana) in 2012 — not a foreign company entering India, but an Indian company that later obtained a Singapore parent structure
- The company obtained Singapore incorporation to attract global investment and benefit from Singapore's business-friendly environment while maintaining Indian operations
- As of 2018: 11 countries, 100+ clients, 100+ employees, covering 13,000+ ads across 400 channels per day
- Clients in India include BMW, CISCO, Volkswagen, Nestle, Domino's, Myntra, Samsung, Airtel
- The company was operating ultrasonic tracking in India from 2014 to at least 2017 — with NO equivalent of the FTC warning issued by any Indian regulatory body

## 4.2 Legal Framework Gaps — Why India Failed to Act (2012–2023)

### Pre-2023: The Legal Vacuum

- India had no dedicated data protection law until 2023. The only applicable provision was Section 43A of the Information Technology Act, 2000 (as amended 2008) — which imposed a 'reasonable security practices' standard that was never enforced against adtech companies.
- The IT (Amendment) Act 2008 and Sensitive Personal Data Rules 2011 were inadequate: they applied only to 'sensitive personal data' (defined narrowly) and provided for civil suits — not regulatory enforcement. No adtech company was ever prosecuted under these rules.
- India had no equivalent of the FTC — no sector-regulator with enforcement authority over adtech privacy violations.
- TRAI (Telecom Regulatory Authority of India) issued a 'Recommendations on Privacy, Security and Ownership of the Data in the Telecom Sector' in 2018 but had no enforcement power over app-based data collection.
- MeITY (Ministry of Electronics and IT) repeatedly deferred a data protection bill from 2017 onward — allowing a 6-year legislative gap during which SilverPush and InMobi operated freely in India.

### The Timeline of India's Failed Legislative Attempts:

| | |
|---|---|
| **2017** | Justice Srikrishna Committee constituted to draft data protection law (after Supreme Court's Puttaswamy privacy judgment) |

| | |
|---|---|
| **2018** | Personal Data Protection Bill draft released — never enacted |
| **2019** | PDP Bill 2019 introduced in Parliament — referred to Joint Parliamentary Committee (JPC) |
| **2021** | JPC submits report with 81 amendments — bill still not enacted |
| **2022** | Government WITHDREW the 2019 PDP Bill entirely in August 2022 — citing need for comprehensive revision |
| **August 2023** | Digital Personal Data Protection (DPDP) Act 2023 receives Presidential assent — FINALLY enacted. However, rules not notified. |
| **Nov 2025** | DPDP Rules 2025 notified by MeITY — Full compliance deadline: May 2027 |
| **TOTAL GAP** | 11+ years from first Supreme Court privacy recognition (2012) to enforceable data protection rules (2025). SilverPush operated during THIS ENTIRE PERIOD without regulatory challenge in India. |

## 4.3 Rise of Cyber Crime Linked to Data Harvesting Ecosystem

India's cybercrime landscape saw dramatic escalation during the period SilverPush and similar adtech companies operated without oversight:

- Cybersecurity incidents in India increased from approximately 1.03 million in 2022 to 2.27 million in 2024 — a 120% increase (Source: DPDP Rules 2025 Compliance Analysis, Scrut.io)
- Behavioral data harvested by adtech SDKs — device IDs, location patterns, network identifiers, browsing behavior — is precisely the data used in targeted phishing, SIM-swap fraud, identity theft, and financial fraud
- The 'audience genome' profiles built by SilverPush represent comprehensive identity dossiers that, if breached or sold, enable criminals to craft highly personalized social engineering attacks
- India's 2022–2024 surge in 'cyber fraud' crimes (phone fraud, OTP fraud, loan app scams) correlates with the maturation of behavioral data ecosystems created by companies like SilverPush

**HIGH RISK FINDING FOR INDIA**
SilverPush's SDK was embedded in hundreds of apps used by Indian consumers. The ultrasonic beacon technology accessed microphones on devices belonging to Indian users — including in apps used by children — without any consent mechanism. This constitutes mass covert surveillance of Indian citizens. Between 2014 and 2023, there was NO Indian law that could have been invoked to prosecute this. Even today, enforcement is untested.

## 4.4 Why Government Policy Failed — Structural Analysis

- LOBBYING CAPTURE: The Indian adtech and digital advertising industry (MMA Global India, IAMAI — Internet and Mobile Association of India) successfully lobbied for light-touch regulation. SilverPush CEO Hitesh Chawla is a regular MMA Global speaker.
- JURISDICTION ARBITRAGE: By registering the parent entity in Singapore while maintaining Indian operations, SilverPush created a structure where: Indian authorities could claim the Singapore entity is out of their jurisdiction; Singapore authorities could claim Indian operations are out of their remit.
- REGULATORY SILOS: MeITY (tech regulation), TRAI (telecom), CCI (competition), and SEBI (if listed) each have partial oversight but no single agency had comprehensive adtech enforcement authority.
- NO WHISTLEBLOWER MECHANISM: India lacked a mechanism for app users or researchers to formally report SDK-level covert data collection to any authority with power to investigate.
- ENFORCEMENT CAPACITY GAP: Indian law enforcement agencies lack dedicated digital forensics capacity to analyze SDK-level tracking — unlike the FTC which has technical staff capable of performing app analysis.
- DPDP ACT LOOPHOLES: Even the new DPDP Act 2023/Rules 2025 contain exemptions for 'legitimate uses' and 'national security' that are vaguely defined. The Data Protection Board of India has not yet demonstrated enforcement capacity.

# SECTION 5: PROSECUTION FRAMEWORK — ESTABLISHING MODUS OPERANDI

## 5.1 Elements Required for Prosecution

### A. Covert Surveillance / Unauthorized Data Collection

- Applicable Law (India): Section 66 IT Act 2000 (computer-related offences); Section 43 IT Act (unauthorized access to computer); Section 72 IT Act (breach of confidentiality); after 2023: DPDP Act Sections 5, 6, 8
- Evidence: FTC documentation showing SDK accessed microphone without disclosure; 234 apps identified by TU Braunschweig in 2017; app code analysis by Kevin Finisterre (Digital Munition) published on GitHub
- Standard: Need to establish that (a) microphone access occurred, (b) without user consent, (c) data was transmitted, (d) SilverPush was the controller

### B. Fraud / Deceptive Practices

- Applicable Law: Section 420 IPC (cheating); Section 468 IPC (forgery for purpose of cheating); Consumer Protection Act 2019
- Evidence: SilverPush's March 2016 public statement claiming discontinuation of audio beacons vs. continued advertising of the service on their website; 2017 research showing 234 apps STILL using beacons; app developer representations to users that apps did not conduct surveillance

### C. Privacy Violation

- Applicable Law (Post-2023): DPDP Act 2023 Section 5 (consent), Section 6 (notice), Section 8 (obligation on data fiduciary); Section 9 (children's data — age 18 in India vs. 13 in US)
- Penalty: Up to INR 250 crore per violation under DPDP Act

## 5.2 Verifiable Sources for Court Use

| | |
|---|---|
| **FTC Warning Letters (2016)** | https://www.ftc.gov/news-events/news/press-releases/2016/03/ftc-issues-warning-letters-app-developers-using-silverpush-code |
| **FTC Sample Warning Letter** | https://www.ftc.gov/system/files/attachments/press-releases/ftc-issues-warning-letters-app-developers-using-silverpush-code/160317samplesilverpushltr.pdf |
| **InMobi FTC Settlement** | https://www.ftc.gov/news-events/news/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked-hundreds-millions-consumers |

| | |
|---|---|
| **MCA Company Record** | Ministry of Corporate Affairs — CIN: U72900DL2012PTC242716 — https://www.mca.gov.in |
| **Bloomberg LEI Record** | https://lei.bloomberg.com/leis/view/984500C56C670FBD0484 |
| **FOIA Records (App List)** | https://altmode.org/2016/07/06/the-ftc-silverpush-warning-letters/ (lists apps via FTC FOIA response) |
| **Security Affairs Technical** | https://securityaffairs.com/42129/hacking/silverpush-technology.html (technical SDK analysis) |
| **Wikipedia / Academic** | https://en.wikipedia.org/wiki/SilverPush (citations to UCL/UCSB/TU Braunschweig research) |
| **CDT FTC Comments (2015)** | Center for Democracy and Technology — FTC Cross-Device Tracking Workshop submission, October 2015 |
| **JM Financial Press Release** | https://jmfl.com/media-center/press-release-detail-home?id=1104 (confirms INR 950M Series C, director Siddharth Kothari) |
| **DPDP Rules 2025** | https://egazette.gov.in/ — G.S.R. 846(E), notified November 13–14, 2025 |
| **Tracxn — Corporate Data** | https://tracxn.com/d/legal-entities/india/silveredge-technologies-private-limited (directors, GST, shareholders) |
| **Zauba Corp — Directors** | https://www.zaubacorp.com/SILVEREDGE-TECHNOLOGIES-PRIVATE-LIMITED-U72900DL2012PTC242716 |

## 5.3 Recommended Investigation Steps

- STEP 1: Obtain all MCA filings for CIN U72900DL2012PTC242716 — annual returns, director KYC, shareholder registry, charge documents
- STEP 2: Issue preservation notices to Google LLC (Play Store) for all versions of apps carrying SilverPush SDK from 2014–2017
- STEP 3: Request FTC FOIA records for the 12 app developers warned in 2016 — names were released via FOIA to Altmode.org researcher
- STEP 4: Conduct forensic analysis of SilverPush SDK versions available on GitHub and archived repositories to confirm beacon functionality post-2016
- STEP 5: Issue legal process to SilverPush/SilverEdge Technologies for server logs, data processing agreements, SDK distribution records
- STEP 6: Contact Technical University Braunschweig (Germany) for the 234-app dataset from their 2017 research — check Indian apps in the list
- STEP 7: Examine cross-directorships — Siddharth Kothari (JM Financial) sits on Silveredge board; examine disclosure obligations
- STEP 8: File complaint with Data Protection Board of India (now operational as of Nov 2025) under DPDP Act for current ongoing violations
- STEP 9: Examine Singapore entity through MAS (Monetary Authority of Singapore) and PDPC (Personal Data Protection Commission Singapore) which has enforcement authority over Singapore-registered entities
- STEP 10: Cross-reference India cybercrime complaint database (cybercrime.gov.in) for any complaints naming SilverPush or affiliated apps

**PROSECUTORIAL STRATEGY NOTE**

The strongest available angle for immediate action is the DPDP Act 2023/Rules 2025 — now fully operative. SilverPush's current 'Mirrors' platform still conducts AI-based content analysis of video being viewed, combined with behavioral profiling. Under DPDP Rules, this requires: (1) a standalone consent notice, (2) specific purpose disclosure, (3) data minimization compliance. The company must comply by May 2027 deadline but can be subjected to complaint-driven investigation NOW. A formal complaint to the Data Protection Board of India with evidence of ongoing non-consensual profiling could initiate India's first adtech privacy enforcement action.

# SECTION 6: EXECUTIVE SUMMARY FOR PROSECUTION

This dossier establishes the following for investigative purposes:

| | |
|---|---|
| 1 | IDENTITY CONFIRMED: Silverpush is legally 'Silveredge Technologies Pvt. Ltd.' (CIN: U72900DL2012PTC242716), incorporated India 25 Sept 2012, HQ Gurgaon, with Singapore parent entity. Founder: Hitesh Chawla (IIT Delhi). Current directors on record. |
| 2 | COVERT SURVEILLANCE CONFIRMED: SilverPush SDK activated device microphones without user knowledge or consent; operated in background; detected inaudible ultrasonic beacons; transmitted behavioral data to remote servers. Confirmed by FTC (2016) and multiple academic studies. |
| 3 | DECEPTION CONFIRMED: Public discontinuation announcement (March 2016) contradicted by (a) continued website advertising of the service, (b) 234 apps still found using beacons in 2017. Pattern of false regulatory statements established. |
| 4 | REGULATORY FAILURE DOCUMENTED: India had no enforceable data protection law from 2012 to 2023 — an 11-year gap. SilverPush operated ultrasonic surveillance in India with ZERO regulatory challenge. India's failure was structural, legislative, and capacity-based. |
| 5 | JURISDICTION PATH: MCA (India) for corporate compliance, Data Protection Board of India (operational Nov 2025) for DPDP Act violations, PDPC (Singapore) for Singapore entity, FTC model serves as evidentiary template for prosecution strategy. |

*All sources cited in this dossier are publicly verifiable through official government records (MCA, FTC, Bloomberg LEI, court documents) and peer-reviewed academic publications. This dossier is intended to support the work of authorized law enforcement and investigative officers in establishing a prosecutable case against digital adtech companies engaging in covert data harvesting operations.*

**— END OF DOSSIER —**

CONFIDENTIAL — FOR AUTHORIZED LAW ENFORCEMENT USE ONLY