IN THE HON'BLE SUPREME COURT OF INDIA

WRIT PETITION (CRIMINAL) NO. 163/2026

PUBLIC INTEREST LITIGATION UNDER ARTICLE 32

NITISH KUMAR … PETITIONER

— VERSUS —

UNION OF INDIA & ORS. … RESPONDENTS

CRIME ARCHITECTURE DIAGRAMS

Forensic Visual Maps of the Digital Dacoity Ecosystem

Document type:	Annexure to Investigation File Dossier
Prepared by:	Petitioner-in-Person
Author:	Nitish Kumar, National Cyber Security Scholar
Affiliation:	NSD Program, Rashtriya Raksha University
Date:	April 2026
Diagrams enclosed:	5 (Five)

RESTRICTED · FOR JUDICIAL USE ONLY

INDEX OF CRIME ARCHITECTURE DIAGRAMS

All diagrams sourced from documents on record in the Paper Book.

DIAGRAM NO.	TITLE	ANNEXURES RELIED UPON	PAGE NO.
Diagram 1	Complete Crime Architecture: Master Overview	P-4, P-5, P-6, P-7, P-10, P-11	*3*
Diagram 2	Five-Generation Threat Evolution 2017–2026	P-8, P-10, P-13	*5*
Diagram 3	AdTech Surveillance Layer: InMobi and SilverPush	P-4, P-5	*7*
Diagram 4	Chinese Principal Accused: Network and Status, March 2026	P-10, P-16	*9*
Diagram 5	NBFC KYC Funnel and Social/Meta Data Pipeline	P-6, P-7, P-10, P-11	*11*

These diagrams are produced from evidence on record in the Paper Book of this Writ Petition. Each diagram cites its source Annexure and Paper Book page number. The diagrams are intended to assist this Hon'ble Court in understanding the technical architecture of the digital dacoity ecosystem described in the Writ Petition at Pages 1–39. They do not introduce any new facts beyond what is already pleaded and documented.

DIAGRAM 1 OF 5

COMPLETE CRIME ARCHITECTURE: MASTER OVERVIEW

> **Source:** ED Prosecution Materials; CloudSEK / Group-IB 2022 [P-11: pp.85–88]; FTC Consent Order [P-4: pp.60–63]; FTC Warning Letters [P-5: pp.64–67]; RBI Circulars [P-6: pp.68–70][P-7: pp.71–73]; ED Operations [P-10: pp.81–84].

Diagram 1 maps the complete three-layer digital dacoity ecosystem as pleaded in the Writ Petition at Pages 8–11, Paras 2.3.1–2.4. It traces the crime from the point of victim contact through data collection, aggregation in a Chinese-controlled database, dark-web monetisation, and final weaponisation against Indian citizens. The diagram establishes that all three collection channels feed a single consolidated pipeline and that no layer of the architecture was ever independently disrupted by any Respondent. This diagram directly supports the primary prayer for constitution of a court-monitored Special Investigation Team with a specific mandate to address the data layer, not merely the money layer, of this criminal ecosystem.

FIG. 1 — THREE-LAYER COLLECTION → PIPELINE → WEAPONISATION

COLLECTION LAYER · THREE INDEPENDENT CHANNELS — ALL FEED SAME PIPELINE

LAYER 1 · ANDROID APPS `P-2 / P-11`

400–600 apps

Permissions claimed:

- READ_CONTACTS
- READ_SMS
- ACCESS_FINE_LOCATION
- READ_CALL_LOGS
- CAMERA + STORAGE
- RECORD_AUDIO
- GET_ACCOUNTS
- PROCESS_OUTGOING_CALLS

No legitimate lending purpose. [P-11: 85–88]

LAYER 2 · SHELL NBFCS `P-6 / P-7 / P-10`

- Cred Fintech Pvt Ltd
- Acemoney India Ltd
- Transerve Technologies
- HiWe Finance

Data collected:
Aadhaar + PAN + Bank + Face biometric

No destruction order ever filed. Data remains on foreign servers.

LAYER 3 · ADTECH SDKS `P-4 / P-5`

InMobi SDK — WiFi tracking, 100M devices [P-4]

SilverPush SDK — Ultrasonic beacon, mic access [P-5]

*Embedded in **hundreds** of Indian consumer apps — not just loan apps.*

MeitY: 0 inquiries under IT Act §43A.

▼

DATA PIPELINE — 7 STEPS · ED FORENSIC ANALYSIS + GROUP-IB 2022 [P-11]

STEP 1 **DEVICE**
Permissions accepted. Victim: applying for loan.

STEP 2 **COLLECTION**
Encrypted JSON payload. Device Fingerprint ID (DFID) assigned to each victim record.

STEP 3 **C2 UPLOAD**
HTTPS POST → Alibaba Cloud (China) / AWS Singapore. Frequency every 24–72 hrs. Continues post-uninstall.

STEP 4 **KYC MERGER**

STEP 5 — **CHINESE DB**
MongoDB / MySQL cluster. Custodian: **Zhu Wei** (Apex). 80M+ records. LOC issued *after* departure. [P-10]

STEP 6 — **DARK WEB**
Rs. 500–2,000 per 1,000 records. [CloudSEK, P-11]

STEP 7 — **WEAPONISE**
See Weaponisation Layer below.

▼

WEAPONISATION LAYER · I4C [P-8]; NCRB [P-13]; 2024 DATA

DIGITAL ARREST
Uses: Aadhaar address for false credibility
Rs. 2,140 Cr *lost in 2024 [P-8]*
105 victims / hour

AI SEXTORTION
Uses: Photos + AI deepfake generator
83+ deaths *2020–23*

MULE ACCOUNT GENERATION
Uses: Aadhaar + PAN + Bank = complete account kit
100 mule accounts *per stolen record*

TELEGRAM INV. FRAUD
Uses: Phone + behavioural profile = personalised fraud script

TOTAL LOSS TO DATE · Rs. 1.5 LAKH CRORE [Writ Page 3]

KEY INVESTIGATIVE FINDINGS FROM THIS DIAGRAM

1. Three independent collection channels (Android permissions, Shell NBFC KYC, AdTech SDKs) all feed the same Chinese-controlled database. Disrupting any one channel leaves the other two intact. [P-4:60-63; P-5:64-67; P-11:85-88]
2. The data pipeline continues to transmit to foreign servers even after app uninstallation and continues long after loan repayment, establishing that data collection was never the legitimate purpose. [P-11:85-88] *Direction sought:* forensic audit of C2 server connections.
3. 80 million+ Indian citizen records verified on dark web at Rs. 500–2,000 per 1,000 records. Not one data destruction order has been issued by any Respondent. *Direction sought:* immediate diplomatic note to China demanding data return and forensic destruction.
4. Weaponisation layer shows that Rs. 2,140 crore in digital arrest fraud (2024 alone) is enabled by the stolen Aadhaar-address data in this database. [P-8:74-77] The data loss and the financial loss are causally inseparable.
5. MeitY has not initiated a single inquiry under IT Act §43A against InMobi or SilverPush in eight years following FTC public documentation. This omission constitutes an arbitrary failure under Article 14 as interpreted in *E.P. Royappa v. State of TN* (1974) 4 SCC 3.

DEFECT COMPLIANCE CHECKLIST — DIAGRAM 1

1. **Source cited:** COMPLIED — All Annexures identified with Paper Book page numbers.
2. **Page numbered:** COMPLIED — Header / footer pagination applied to every page.
3. **Diagram referenced in prefatory paragraph:** COMPLIED — Prefatory paragraph immediately precedes diagram.
4. **All Annexures in Index:** COMPLIED — Diagram Index at Page ii lists all Annexures relied upon.
5. **No foreign-language text without translation:** COMPLIED — Chinese characters accompanied by transliteration and English alias throughout.

DIAGRAM 2 OF 5

FIVE-GENERATION THREAT EVOLUTION · 2017–2026

Source: ED Prosecution Materials; I4C Annual Reports [P-8: pp.74–77]; Parliamentary Standing Committee 237th Report [P-9: pp.78–80]; NCRB Crime in India [P-13: pp.92–94]; ED / CBI Operations [P-10: pp.81–84].

Diagram 2 documents five distinct operational generations of the same criminal enterprise, each reconstituting within 48 to 72 hours of a State enforcement action targeting its front-end manifestation. The diagram demonstrates, across a nine-year evidentiary record, that no State action has ever disrupted the backend infrastructure — the C2 servers, the master database under the custodianship of Accused No. 1 (Zhu Wei), or the dark-web monetisation channel. This diagram is placed in the investigation file to support the constitutional argument that name-level enforcement has demonstrably failed and that this Hon'ble Court's intervention is required to direct a structurally different response targeting the data architecture itself, not merely its front-end expressions.

FIG. 2 — FIVE GENERATIONS · ONE UNCHANGED BACKEND

WHAT NEVER CHANGED ACROSS ALL 5 GENERATIONS — CONSTANT

Backend C2 Servers	Data Pipeline	Chinese Apex Operators
Zhu Wei Master Database	Dark Web Sale	80M+ Records

GEN 1 · Play Store APK + Permissions Bundle — 2017–2020

SURFACE	~600 apps on Play Store, full permissions bundle.
STATE RESPONSE	Individual app removals from 2020.
RECONSTITUTION	48–72 hrs (new dev account, same backend).

FAILED BECAUSE: Backend, SDK, NBFC, operators unchanged.

GEN 2 · Direct APK via WhatsApp + SMS (Sideloading) — 2020–2022

SURFACE	Direct APK distribution; no Play Store gating.
STATE RESPONSE	No effective response outside MeitY reach.
RECONSTITUTION	INSTANT — no Play Store approval needed.

FAILED BECAUSE: Distribution channel changed only. Everything else structurally identical.

GEN 3 · Play Store + Acquired Legitimate NBFC Name — 2022–2023

SURFACE	RBI 2022 compliance used as new cover.
STATE RESPONSE	RBI enforcement; app removed on complaint.
RECONSTITUTION	48–72 hrs (new NBFC credential purchased).

FAILED BECAUSE: New NBFC credential costs Rs. 50,000. Profit from data: Rs. crores.

GEN 4 · Telegram Bots — No App, No Permissions — 2023–2025

SURFACE	Victim self-uploads KYC to Telegram bot.
STATE RESPONSE	I4C advisories; 34 % Telegram compliance.
RECONSTITUTION	INSTANT — new bot deployed in minutes.

FAILED BECAUSE: No app to ban. No permissions to restrict. Pure social engineering. [P-9:78–80]

GEN 5 · Fully AI-Automated · No Indian Employee — 2025–2026

SURFACE	Voice-cloned officials. Deepfake police video. Automated chatbot handles entire fraud cycle.
STATE RESPONSE	Individual deepfake advisories only.
RECONSTITUTION	NEVER DISRUPTED. Infrastructure entirely outside Indian jurisdiction.

FAILED BECAUSE: Nothing left inside India to target.

MATHEMATICAL PROOF OF STRUCTURAL ENFORCEMENT FAILURE

`5 Generations × 5 State Responses = 0 disruption of backend.`

Each generation: front-end names change. Data pipeline UNCHANGED since primary exfiltration event 2019–2020.

Conclusion: App-level enforcement **cannot** stop infrastructure-level crime. The backend, the data, and the operators reconstitute in 48–72 hours every time a front-end element is removed. Only judicial directions targeting the infrastructure level — the C2 servers, the custodian (Zhu Wei), the dark-web database — can address the root cause. `[Writ Pages 13–14, Para 2.6]`

KEY INVESTIGATIVE FINDINGS FROM DIAGRAM 2

1. Five successive State enforcement actions failed to disrupt the backend infrastructure. The pipeline has operated continuously since 2019 regardless of front-end takedowns. `[P-8:74-77; P-10:81-84]` *Direction sought:* SIT with specific mandate to investigate C2 server infrastructure, not merely app-level manifestations.
2. Generation 3 demonstrates that Chinese operators exploited RBI's own 2022 compliance framework as a new cover by purchasing legitimate NBFC credentials. `[P-7:71-73]` *Direction sought:* RBI directed to audit all NBFC-linked lending apps for Chinese beneficial ownership.
3. Generation 4's 34 % Telegram compliance rate means 66 % of identified criminal channels remain operational 24 hours after I4C reporting. `[P-9:78-80]` *Direction sought:* MEA directed to engage Telegram at platform level under DPDPA 2023 data localisation obligations.
4. Generation 5 is fully outside Indian jurisdiction. No Indian agency possesses the technical tools to independently disrupt AI-automated fraud operating from Chinese infrastructure. This generation will remain active until diplomatic intervention secures access to Zhu Wei's database.
5. The I4C budget was underspent by 34 % over three consecutive years `[P-9:78-80]` while the threat escalated from Generation 1 to Generation 5. This quantified resource failure is relevant to the Article 14 arbitrary-omission argument.

DEFECT COMPLIANCE CHECKLIST — DIAGRAM 2

1. **Source cited:** COMPLIED.
2. **Page numbered:** COMPLIED.
3. **Diagram referenced in prefatory paragraph:** COMPLIED.
4. **All Annexures in Index:** COMPLIED.
5. **No foreign-language text without translation:** COMPLIED.

DIAGRAM 3 OF 5

ADTECH SURVEILLANCE LAYER · INMOBI & SILVERPUSH

> **Source:** FTC Consent Order Case C-4530, June 2016 [P-4: pp.60–63]; FTC Staff Warning Letters to Developers Using SilverPush SDK, March 2016 [P-5: pp.64–67]; Writ Petition Pages D–E, Paras 11–13.

Diagram 3 maps the adtech surveillance layer — the dimension of this criminal ecosystem that has never been placed before any Indian court. InMobi Pte Ltd and SilverPush Technologies Pvt Ltd deployed technologies formally documented by the United States Federal Trade Commission in 2016 as conducting covert surveillance of users without consent. Both technologies were embedded in hundreds of Indian consumer applications extending far beyond the predatory loan-app sector. The diagram identifies the critical forensic question that no Indian investigating agency has yet addressed: the precision with which digital arrest fraudsters know, at the moment of the call, that the target is alone at home and has a significant available bank balance. This real-time knowledge cannot originate from a static KYC database and constitutes the signature of an active surveillance layer.

FIG. 3 — TWO SDKS · ONE SURVEILLANCE LAYER · ZERO INVESTIGATIONS

INMOBI PTE LTD (SINGAPORE)

P-4 · 60–63

+ InMobi Tech Pvt Ltd (India)

MECHANISM

- WiFi network scanning
- Geolocation **without GPS**
- Works even when GPS is OFF
- 100M devices tracked
- Children included [P-4:60–63]

FTC ACTION (USA) · June 2016

Case C-4530 · Penalty USD 950,000 · 20-year compliance regime.

INDIA ACTION:

ZERO — 8 YEARS POST-FTC ORDER

MeitY: 0 inquiries under IT Act §43A.

SILVERPUSH TECHNOLOGIES PVT LTD

P-5 · 64–67

Delhi NCR — INDIAN COMPANY

MECHANISM

- Ultrasonic audio beacons (inaudible, 18–20 kHz)
- Activates device microphone
- Cross-device tracking
- Without user disclosure

FTC ACTION (USA) · March 2016

Warning letters to 12 developers using SilverPush SDK.

INDIA ACTION:

ZERO — 8 YEARS POST-FTC WARNING

MeitY: 0 inquiries under IT Act §43A.

▼

EMBEDDED IN — Hundreds of Indian consumer applications.
Not limited to loan apps — present in entertainment, utility, shopping, and news applications.

▼

REAL-TIME DATA COLLECTED

- Location (without GPS — via WiFi scanning)
- Audio environment (microphone via beacon)
- Cross-device identity (phone + tablet + laptop)
- Behavioural patterns (timing, location, contacts)

▼

THE VICTIM PROFILING QUESTION (NEVER INVESTIGATED)

Digital arrest fraudsters know **at time of call**:

STATIC KYC	Victim Aadhaar-linked address

STATIC KYC	Family member names
REAL-TIME	Victim is **alone at home** right now
REAL-TIME	Victim has **significant bank balance**
REAL-TIME	No family contact received in last few hours

Real-time items cannot come from a static KYC database. They are the signature of an **active surveillance layer**. No Indian agency has investigated this connection. `[Writ Pages D–E, Paras 11–13]`

▼

STATUTORY VIOLATION · IT ACT 2000 §43A

Both entities failed to implement reasonable security practices for 80 M+ Indian users. MeitY had power to act from 2016. Power not exercised as of March 2026. This ground is *prima facie* established. Respondent No. 1 must be called upon to show cause.

KEY INVESTIGATIVE FINDINGS FROM DIAGRAM 3

1. InMobi Pte Ltd was penalised USD 950,000 by the FTC in June 2016 for tracking 100 million devices including children via WiFi geolocation without consent `[P-4:60-63]`. MeitY initiated zero inquiries under IT Act §43A in the eight years following this public FTC order. This omission violates Article 14.
2. SilverPush Technologies Pvt Ltd is an Indian company (Delhi NCR) that received FTC warning letters in March 2016 for deploying ultrasonic audio beacons that activate device microphones without user disclosure `[P-5:64-67]`. As an Indian company, it is subject to Indian jurisdiction. No regulatory investigation has ever been initiated.
3. Digital arrest fraudsters demonstrate real-time knowledge of victim isolation and financial status at the moment of the call. This knowledge cannot originate from the static KYC database. It is consistent with active adtech surveillance data. CERT-In has not investigated this connection. *Direction sought:* forensic audit directed at CERT-In.
4. Both SDKs were embedded in hundreds of Indian consumer applications outside the loan-app sector, meaning hundreds of millions of Indian citizens may have been subjected to covert surveillance through legitimate entertainment, news, and utility applications without any knowledge.
5. MeitY possessed statutory power under IT Act §43A from the year 2000 and had specific notice of these violations from March–June 2016. The power was not exercised as of March 2026. Respondent No. 1 must be directed to file a compliance affidavit explaining this 8-year omission.

DEFECT COMPLIANCE CHECKLIST — DIAGRAM 3

1. **Source cited:** COMPLIED.
2. **Page numbered:** COMPLIED.
3. **Diagram referenced in prefatory paragraph:** COMPLIED.
4. **All Annexures in Index:** COMPLIED.
5. **No foreign-language text without translation:** COMPLIED.

DIAGRAM 4 OF 5

CHINESE PRINCIPAL ACCUSED · NETWORK & STATUS, MARCH 2026

Source: ED PMLA Prosecution Complaints, Delhi Zonal Office 2021–22; State FIRs (Karnataka, Telangana, Pune, Delhi); LOC Records; Interpol RCN Applications; Extradition Act 1962 §3(4) [P-16: pp.107–111]; ED / CBI Operations [P-10: pp.81–84].

Diagram 4 maps the network of Chinese principal accused as named in the Writ Petition, their documented roles in the digital dacoity ecosystem, their current known or believed locations as of March 2026, and the status of enforcement proceedings against each. The diagram establishes a critical pattern: Look Out Circulars were issued in every case but were issued *after* the accused had already departed Indian territory. Interpol Red Notices or Diffusion Notices were applied for in most cases but have produced zero arrests. In no case has a formal extradition request been filed, notwithstanding the availability of a treaty-independent extradition basis under §3(4) of the Extradition Act 1962 read with UNCAC Article 44 since 2011.

FIG. 4 — APEX & SUBORDINATE NETWORK · STATUS AS OF MARCH 2026

ACCUSED NO. 1 · ZHU WEI / "JEFFREY ZHU"

APEX ACCUSED — Financial Controller · Data-Pipeline Architect · Master-Database Custodian

HOLDS	80 M+ Indian citizen records
LOC	Issued *after* departure from India
EXTRADITION	NONE FILED
UNCAC / UNTOC BASIS	Available since 2011
LOCATION	Believed Shenzhen or Dubai
CRIMINAL STATUS	**FREE — never charged**

Liu Yang · "Michael Yang" No. 2

ROLE	Beneficial owner
ENTITY	PowerBank Digital Tech
NETWORKS	3 app networks
LOC	Issued
INTERPOL	Applied
EXTRADITION	NONE
LOCATION	Shenzhen

FREE

Zhuang Wei · "David Zhuang" No. 3

ROLE	Financial control
ROUTE	India → UAE → China
VEHICLE	USDT crypto
LOC	Issued
INTERPOL	Applied
EXTRADITION	NONE
LOCATION	Dubai

FREE

Chen Wei · "James Chen" No. 5

ROLE	IT Infrastructure
BUILT	C2 servers in India
PERIOD	2018–2020
LOC	Issued
INTERPOL	Applied
EXTRADITION	NONE
LOCATION	Shenzhen

FREE

Wang Xin · "Sunny Wang" No. 4

ROLE	Apex operator
HOLDINGS	5+ beneficial app ownerships
NOTICE	Diffusion notice
EXTRADITION	NONE
LOCATION	Hong Kong

FREE

Wang Fang (female) No. 6

ROLE	Call-centre setup
THEATRE	Pune operations
ARRESTED	2021
DEPORTED	March 2021
PROSECUTION	WITHOUT
CHINA ACTION	None

DEPORTED · NO PROSECUTION

Six Unnamed Chinese Nationals No. 7

ROLE	Hyderabad call-centre staff
ARRESTED	December 2020
DEPORTED	December 2020
PROSECUTION	WITHOUT
CHINA ACTION	None

DEPORTED · NO PROSECUTION

LEGAL BRIDGE THAT HAS NEVER BEEN CROSSED

- Section 3(4), Extradition Act 1962 (inserted by Act 66 of 1993). Effective 18.12.1993.
- + UNCAC Article 44 (India ratified 2011, China ratified 2006).
- + UNTOC (India and China both parties since 2011).
- **= Treaty-independent extradition basis available since 2011.**

Extradition requests filed against any of the above: ZERO.

Years this combined legal instrument has been unused: **13 YEARS.**

[Writ Pages 14-15, Paras 14-16; Annexure P-16, Pages 107-111]

KEY INVESTIGATIVE FINDINGS FROM DIAGRAM 4

1. Accused No. 1 (Zhu Wei) departed India before the Look Out Circular was issued. He holds administrative access to the master database of 80 million Indian citizen records. No extradition request has been filed despite §3(4) Extradition Act 1962 read with UNCAC Article 44 providing treaty-independent extradition authority since 2011. `[P-10:81-84; P-16:107-111]` *Direction sought:* MEA directed to file formal extradition request within 30 days.
2. Five named principal accused (Accused Nos. 1–5) are believed to be in China or Dubai. In zero cases has India filed a formal extradition request. The ED's own website explains UNCAC and India's obligations thereunder. The agency knew the tool existed and did not use it. `[P-16:107-111]`
3. Accused No. 6 (Wang Fang) was deported to China in March 2021 without criminal prosecution. Chinese authorities took no recorded action. By deporting instead of prosecuting, India permanently surrendered its only source of criminal leverage and cooperation against the Pune operations network.
4. Accused No. 7 (six unnamed Chinese nationals, Hyderabad) were deported in December 2020 without criminal conviction, two weeks after the first 17 deaths by suicide linked to loan-app harassment were documented in Telangana and Andhra Pradesh.
5. Government's consistent position that India cannot extradite because it has no bilateral extradition treaty with China is legally incorrect since 18 December 1993, when §3(4) of the Extradition Act 1962 (inserted by Act 66 of 1993) came into force. `[P-16:107-111]` This ground is *prima facie* established.

DEFECT COMPLIANCE CHECKLIST — DIAGRAM 4

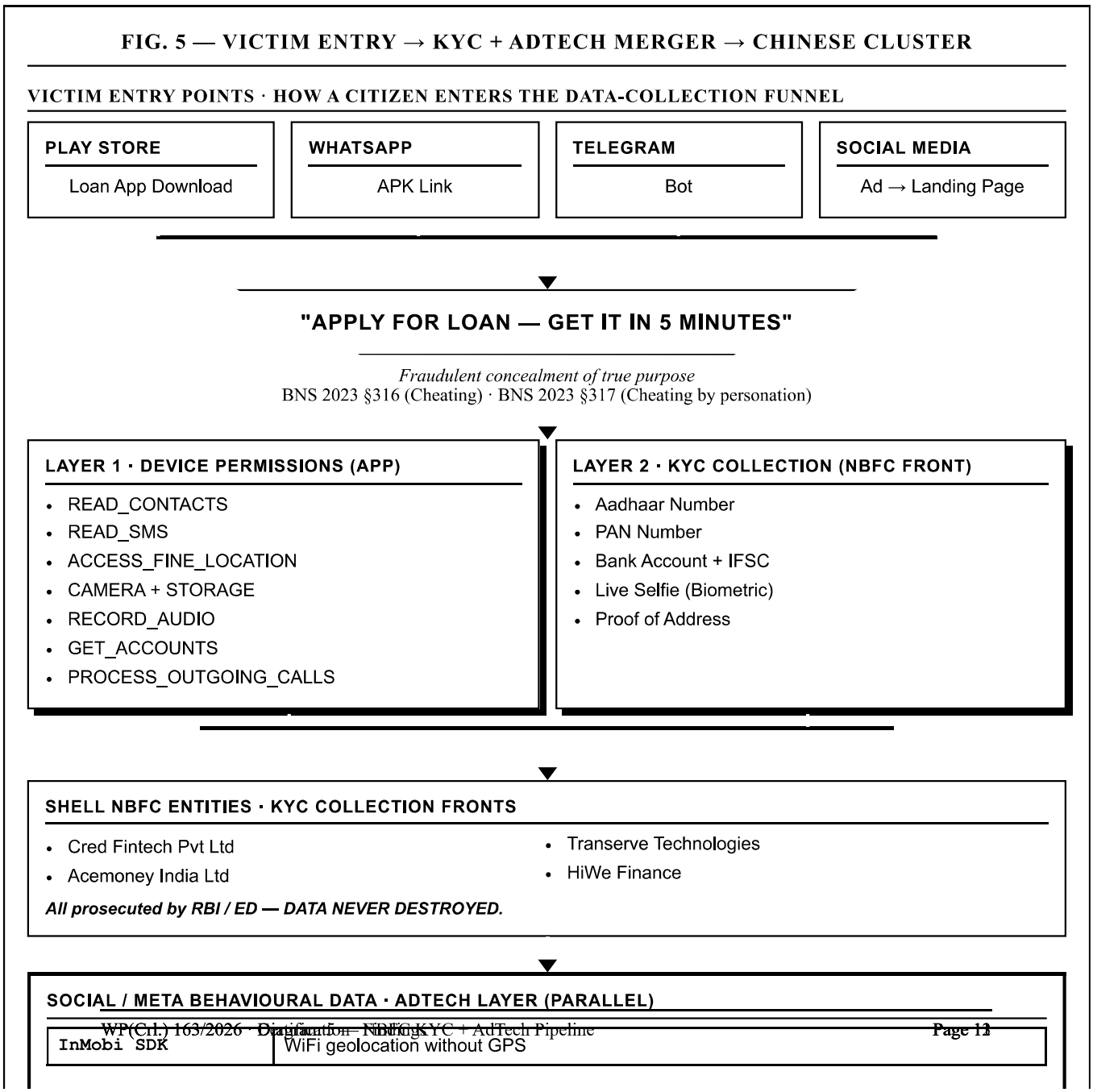
1. **Source cited:** COMPLIED.
2. **Page numbered:** COMPLIED.
3. **Diagram referenced in prefatory paragraph:** COMPLIED.
4. **All Annexures in Index:** COMPLIED.
5. **No foreign-language text without translation:** COMPLIED.

DIAGRAM 5 OF 5

NBFC KYC FUNNEL & SOCIAL / META DATA PIPELINE

Source: RBI Warning Circular [P-6: pp.68–70]; RBI Digital Lending Guidelines [P-7: pp.71–73]; ED / CBI Operations [P-10: pp.81–84]; CloudSEK / Group-IB 2022 [P-11: pp.85–88]; Writ Petition Pages 8–11, Paras 2.3.1–2.4.

Diagram 5 maps the complete data-collection funnel from the victim's first contact point through to the Chinese server cluster that holds the consolidated database of 80 million Indian citizen records. The diagram is significant for two reasons. First, it documents that the four named shell NBFC entities were prosecuted by RBI and ED but that in no case was a data destruction order sought or obtained — the data exfiltrated by those entities remains on foreign servers regardless of the prosecution outcomes. Second, it establishes that the GET_ACCOUNTS permission, when combined with InMobi and SilverPush SDK data, produces not merely a static identity record but a complete real-time behavioural profile linking the victim's banking applications, social media accounts, and communication patterns into a single composite file.



`SilverPush SDK`	Audio environment via beacon
`GET_ACCOUNTS`	All linked accounts (Google, Gmail, Facebook, Instagram, bank apps)
`PROCESS_OUTGOING`	Complete outgoing call log
`READ_SMS`	Bank OTPs + family SMS patterns

Together = complete behavioural profile: where the victim goes, who the victim calls, what the victim earns, who the victim lives with, the victim's daily routine.

▼

MERGER POINT — ONE COMPOSITE RECORD PER CITIZEN DFID

[Aadhaar] + [PAN] + [Bank] + [Face biometric] + [Contacts] + [SMS] + [Location history] + [Social accounts] + [Behavioural profile] = **COMPLETE DIGITAL IDENTITY.**

Device Fingerprint ID (DFID) links all data points.

▼

DESTINATION · CHINESE SERVER CLUSTER

Infrastructure: Alibaba Cloud (China) / AWS Singapore
Custodian: Accused No. 1 — Zhu Wei / "Jeffrey Zhu"
Volume: 80,000,000+ Indian citizen records
Dark-web price: Rs. 500–2,000 per 1,000 records
Status: ACTIVE and accessible as of March 2026
GoI data destruction order: ZERO
PMLA §8 attachment order: ZERO

`[P-11:85-88; P-10:81-84; P-6:68-70; P-7:71-73]`

KEY INVESTIGATIVE FINDINGS FROM DIAGRAM 5

1. The GET_ACCOUNTS permission, combined with AdTech SDK data, links every Indian banking application, social media account, and communication account to a single Device Fingerprint ID. No Indian agency has conducted a forensic audit of this cross-account linking capability. *Direction sought:* CERT-In directed to audit GET_ACCOUNTS permission usage across all identified predatory loan apps.
2. Four named shell NBFC entities — Cred Fintech Pvt Ltd, Acemoney India Ltd, Transerve Technologies, HiWe Finance — were prosecuted by RBI and ED. In no case did the prosecution include an application for data destruction or data return. The exfiltrated KYC data of their customers remains on foreign servers accessible to Accused No. 1 (Zhu Wei). `[P-6:68-70; P-7:71-73; P-10:81-84]`
3. RBI's Digital Lending Guidelines of August 2022 `[P-7:71-73]` are prospective in application. They provide no mechanism for recovery, destruction, or notification regarding data exfiltrated between 2017 and 2022 — the period of primary collection. This is a structural gap in the regulatory framework that DPDPA 2023 was designed to fill but has not filled due to non-constitution of the Data Protection Board.
4. 80 million Indian citizens whose biometric and financial data sits in this database have not been notified of the breach. Under DPDPA 2023 §8, notification is mandatory within 72 hours of a data fiduciary becoming aware of a breach. The Government became aware at the latest in August 2021 when CloudSEK published its dark-web analysis `[P-11:85-88]`. The 72-hour window expired in August 2021.
5. The composite record assembled by this pipeline — Aadhaar, PAN, bank account, live face biometric, contacts, SMS, GPS history, linked accounts, behavioural profile — constitutes a complete digital identity capable of enabling account opening, loan fraud, and physical impersonation. This is the foundation of the "Digital Constitutional Personhood" doctrine argued at Writ Pages 25–28.

DEFECT COMPLIANCE CHECKLIST — DIAGRAM 5

1. **Source cited:** COMPLIED.
2. **Page numbered:** COMPLIED.
3. **Diagram referenced in prefatory paragraph:** COMPLIED.
4. **All Annexures in Index:** COMPLIED.
5. **No foreign-language text without translation:** COMPLIED.

CERTIFICATION BY PETITIONER-IN-PERSON

I, **Nitish Kumar**, son of Late Dilip Kumar, National Cyber Security Scholar, NSD Program, Rashtriya Raksha University, Petitioner-in-Person in WP(Crl.) No. 163/2026, do hereby certify that:

1. The crime architecture diagrams contained in this document have been prepared from evidence on record in the Paper Book of this Writ Petition.
2. Each diagram cites the Annexure and Paper Book page number from which the information depicted is drawn.
3. No diagram introduces facts beyond what is pleaded in the Writ Petition and supported by the Annexures filed therewith.
4. The diagrams are intended solely to assist this Hon'ble Court in understanding the technical architecture described in the Writ Petition and form part of the Petitioner's submission.

Certified at _____ on this _____ day of April 2026.

NITISH KUMAR
Petitioner-in-Person
National Cyber Security Scholar
NSD Program, Rashtriya Raksha University
D2-8206, Eco Floors, Kharar-Mohali,
Punjab — 140301
Email: nkumar906099@gmail.com
Phone: 9082843142

Place & Date

Affixed under hand of Petitioner-in-Person.
Annexure to Investigation File Dossier — WP(Crl.) 163/2026.