RESEARCH DOSSIER — APRIL 2026

INDIA CYBER CRIME: GOVERNMENT OPEN RECORD, THREAT MODEL GAPS & SOP ARCHITECTURE FAILURES

Prepared for Submission Before the Supreme Court of India

Writ Petition (Criminal) — Public Interest Litigation

Nitish Kumar v. Union of India & Ors.

Petitioner	Nitish Kumar, Petitioner-in-Person
Date	April 2026
Classification	Confidential — For Court Submission Only
Sources	MHA / I4C / NCRB / PIB / Parliamentary Replies / Institutional Research
Sections	7 Sections: Govt. Record | Financial Scale | DPDPA | Threat Model | SOP | Enforcement Gaps | Court Findings

[TOC] TABLE OF CONTENTS

Section 1	Government Open Record — What Has Been Done Till 2026	3
Section 2	Financial Scale of Failure — Official Government Figures	6
Section 3	DPDPA 2023 — Updated Status and Critical Argument Update	7
Section 4	Threat Model — Five Critical Weaknesses	8
Section 5	SOP Architecture — How Each SOP Works and Where It Fails	11
Section 6	Enforcement Gaps — Documented Official Record	14
Section 7	Court-Ready Findings — Updated Arguments for Submission	16
Appendix A	Sources and Official References	18

[01] GOVERNMENT OPEN RECORD — WHAT HAS BEEN DONE TILL 2026

The following constitutes the complete official action log of the Government of India in relation to cyber crime, data protection, and digital fraud enforcement from 2018 to April 2026. All entries are sourced exclusively from official government publications, Parliamentary replies, PIB press releases, and MHA/I4C records. The final row documents actions never taken across this entire period — forming the constitutional accountability gap at the centre of this petition.

1.1 Official Statistics Scorecard

METRIC	FIGURE	SOURCE
SIM Cards Blocked (till 31 Oct 2025)	11.14 lakh	PIB/MHA Dec 2025
IMEI Numbers Blocked	2.96 lakh	PIB/MHA Dec 2025
Money Saved via CFCFRMS (cumulative)	Rs. 7,130 Crore	MHA I4C Oct 2025
Total Cyber Financial Loss 2024	Rs. 22,845 Crore (+206%)	MHA to Parliament 2025
FIR Conversion Rate — National Average (Dec 2025)	2.22%	Centre to States, Apr 2026
1930 Helpline — Daily Calls (2025 average)	88,976 calls / day	I4C 2025 Report
Total 1930 Helpline Calls — Full Year 2025	3.24 crore	I4C 2025 Report
Mule Accounts Frozen (cumulative)	24 lakh+	I4C 2025
Cyber Crime Complaints Registered 2024	22.68 lakh	MHA to Parliament 2025
Cyber Crime Complaints Registered 2025	28.15 lakh	I4C 2025 Annual Data

1.2 Complete Government Action Log — 2018 to 2026

YEAR	ACTION TAKEN	STATUS	CRITICAL GAP — WHAT WAS NOT DONE
2018	I4C Scheme approved. Rs. 415.86 Crore outlay. 7 components: TAU, NCRP, NCFL, NCTC, CFMC, Ecosystem Unit, R&I Centre.	Done	No data pipeline investigation mandate. No SDK audit provision. No foreign server reach mechanism.
2019	National Cyber Forensic Lab (Investigation) established at New Delhi.	Done	Lab serves domestic investigating officers only. Zero mandate to trace data exfiltration to foreign servers.
2020 Jun	59 Chinese apps banned under IT Act S.69A. I4C dedicated to nation by Home Minister.	Partial	SDK components in non-banned apps continued data collection. C2 server pipeline unaffected. No data destruction order. Zero notification to 80 million victims.
2021	1930 Helpline operationalised. CFCFRMS launched to save funds in real time.	Done	Jeffrey Zhu departed India before LOC issued — documented investigative failure. CloudSEK published 80M KYC dark web finding. Government response to data dimension: nil.
2022 Aug	RBI Digital Lending Guidelines — data minimisation mandate, NBFC name on app, cooling off period.	Partial	Prospective only. Zero retrospective provision for 2019-2022 exfiltrated data. No forensic audit of NBFC data storage ordered.
2023 Aug	DPDPA enacted. Creates DPB, 72-hr breach notification obligation, Rs. 250 Crore maximum penalty.	Partial	Board NOT constituted for 27 months post-enactment. Rules not notified till Nov 2025. Zero DPDPA enforcement 2023-2025.
2023-24	Operation Chakra-II (CBI): 43 arrests. Operation Hawk (ED): 60 arrests, Rs. 800 Crore attached.	Partial	ALL 103 arrested = Indian nationals. Zero Chinese principals arrested. Zero extradition request filed. Zero data recovery action. Money followed; data was not.
2024 Jul	I4C upgraded to Attached Office of MHA. AoB Rules amended — NSCS nodal for cybersecurity strategy.	Done	Coordination between MHA (crime), MeitY (data), DoT (telecom) remains fragmented. Carnegie Endowment (Sep 2025): India's organisational measures identified as weakest area.

2024 Nov	Telecom Cyber Security Rules notified. TSPs: 6-hr incident reporting; 24x7 SOC mandatory.	Done	Telecom-layer only. SDK-embedded surveillance in consumer apps not covered. BSNL hack (May 2024) — response prospective only.
2025 Jan	India-US MoU (I4C + DHS) for cybercrime investigation cooperation. Aadhaar authentication extended to private entities.	Done	India-China: ZERO cooperation instrument for cyber fraud. UNCAC Art. 44 still not invoked. Aadhaar extension expands biometric surface without resolving existing pipeline breach.
2025 May	e-Zero FIR introduced — frauds above Rs. 10 lakh auto-register as FIR via 1930 regardless of jurisdiction.	Done	Low-value fraud (under Rs. 10L) — majority of cases — still requires manual FIR at police station. FIR rate dropped to 1.4% provisional in 2025.
2025 Nov	DPDP Rules 2025 notified. DPB establishment provisions in force (Phase I). Full enforcement only by May 2027.	Partial	DPB framework exists but Board members not appointed. Substantive provisions operative only May 2027. 80M breach victims: no notification as of April 2026.
2025-26	CNAP pilot by TRAI. SIM-Binding mandate for messaging apps. Pratibimb criminal mapping module operational.	Partial	CNAP and SIM-Binding in rollout — not yet fully live. Does not address international VoIP (Gen 5 primary channel). Does not address already-exfiltrated data.
NEVER 2012-2026	**Actions never taken across 14 years:**	**NOT DONE**	**1. Extradition request under S.3(4) Extradition Act 1962 against any Chinese national — NEVER FILED 2. Data recovery/destruction note to China, UAE, Cambodia — NEVER ISSUED 3. MLAT request for data on foreign servers — NEVER FILED 4. InMobi/Silverpush investigation under IT Act S.43A — NEVER OPENED 5. Notification to 80M affected citizens of data breach — NEVER ISSUED 6. Forensic investigation targeting data pipeline (not money) — NEVER CONDUCTED 7. Data destruction as condition of PMLA settlement — NEVER SOUGHT**

[02] FINANCIAL SCALE OF FAILURE — OFFICIAL GOVERNMENT FIGURES

The following data is drawn entirely from MHA Parliamentary replies, NCRB Crime in India reports, and I4C Annual Data. These are not estimates by private researchers — they are the government's own numbers submitted before Parliament. The trajectory from 2021 to 2026 establishes that financial losses increased six-fold while FIR conversion rates declined.

YEAR	COMPLAINTS (NCRP)	FINANCIAL LOSS	SAVED / RECOVERED	FIR %
2021	~4.5 lakh	Not separately quantified	Rs. 4,386 Cr (cumulative start)	~2.5%
2022	NCRB: 65,983 FIRs	Rs. 7,465 Cr (est.)	Partial via CFCFRMS	~2.3%
2023	NCRB: 86,420 FIRs (+31%)	Rs. 7,465 Cr (official)	Partial	~2.3%
2024	22.68 lakh complaints	Rs. 22,845 Cr (+206%)	Rs. 7,130 Cr saved (cumul.)	2.9%
2025	28.15 lakh complaints	Rs. 22,495 Cr	Rs. 8,031 Cr saved (cumul.)	1.4% (prov.)
2026 (Proj.)	**Est. 35+ lakh**	**Rs. 1.2 lakh Crore (I4C)**	**—**	**—**

KEY FINDING — SECTION 2

The government cumulatively saved Rs. 8,031 crore via CFCFRMS since 2021. In the same period, total losses exceeded Rs. 45,000+ crore. The money recovery rate in Karnataka — India's most cyber-advanced state — fell below 10% in 2025 despite faster bank response times. Money recovery is happening at the margins. The principal fraud architecture — the data pipeline — remains entirely untouched.

[03] DPDPA 2023 — UPDATED STATUS AND CRITICAL ARGUMENT UPDATE

CRITICAL UPDATE — PETITION ARGUMENT REQUIRES REVISION

The petition (filed March 2026) states the Data Protection Board 'was never constituted.' This is now partially superseded. On 13 November 2025, MeitY notified the DPDP Rules 2025 and brought Phase I (DPB establishment provisions) into force. The Solicitor General will use this to argue the prayer is infructuous. The petitioner must update the argument — the updated version is actually stronger.

PHASE	EFFECTIVE DATE	PROVISIONS ACTIVE	STATUS — APRIL 2026	PETITION IMPACT
Phase I	13 Nov 2025	DPB establishment provisions, Board powers and structure	Board framework legally active. Board members NOT yet appointed. Not operationally functional.	Argument that Board 'never constituted' is outdated. Must shift to operational non-functionality + phased timeline argument.
Phase II	13 Nov 2026	Consent manager registration; Board jurisdiction over consent breaches	7 months away. Not yet operative.	Breach notification jurisdiction for 80M victims still legally inoperative for minimum 7 months.
Phase III	13 May 2027	ALL substantive obligations: consent, breach notification, security, penalties	13 months away. Not yet operative.	Full enforcement regime — penalties, breach notification, data rights — is 13 months away. This is the strongest updated argument.

Updated Petition Argument — Replace Original DPB Prayer With:

UPDATED PRAYER — DPDPA (replaces original DPB non-constitution prayer)

The DPDPA was enacted on 11 August 2023. Rules were notified 27 months later on 13 November 2025. Substantive enforcement provisions — consent, breach notification, and penalties — will only become operative on 13 May 2027, a period of 45 months after enactment. The 80 million Indian citizens whose biometric and financial data was stolen in 2020-2022 will have waited seven (7) years before any statutory breach notification obligation applies to their data. This Court, exercising jurisdiction under Article 32 read with Article 142, has the power and the duty to direct immediate breach notification to these 80 million citizens as an interim constitutional direction — without waiting for a phased statutory timeline designed for prospective commercial compliance, not for victims of a historical data heist of national scale.

[04] THREAT MODEL — FIVE CRITICAL WEAKNESSES

India's cyber crime threat model — as it exists across I4C, CERT-In, DoT, and RBI — is fundamentally built on a transactional harm model. It tracks money flows, phone numbers, and device identifiers. It does not model the data layer. This is the architectural flaw identified in the petition. The following five weakness assessments are based entirely on official government publications, parliamentary replies, and peer-reviewed institutional analysis.

WEAKNESS 1 Data Pipeline Layer — Not Mapped in Any Official Threat Model

Severity: **CRITICAL — NOT ADDRESSED**

India's entire enforcement architecture treats the criminal ecosystem as a financial crime with a digital medium. The actual threat is a data crime with a financial output. The government's threat model tracks: SIM cards to mule accounts to money flows to arrest of mule account holders. What it does NOT track: app installation to device permission exploitation to C2 server upload to NBFC KYC merger to Chinese database to dark web sale to AI-automated weaponisation cycle.

- No agency has mapped the full data pipeline from Android app permissions to Shenzhen server as a connected forensic target.
- CERT-In handled 29.44 lakh cyber incidents in 2025 — zero relate to tracing data exfiltration pipeline architecture.
- Pratibimb module maps Indian criminal locations — does not map Chinese backend servers or SDK data collectors.
- No threat intelligence exchange exists between India and China on data exfiltration specifically.
- Trusted Telecom Portal bans Chinese hardware — Chinese-owned data collection SDKs in consumer apps are not covered.

WEAKNESS 2 Adtech Surveillance Layer — Never Entered Any Indian Threat Model

Severity: **CRITICAL — ABSENT**

India's cyber crime threat model has never included the adtech surveillance layer as a threat vector. Neither I4C, CERT-In, nor MeitY has modelled the InMobi/Silverpush SDK deployment as part of the victim-profiling infrastructure that enables precision targeting in Generation 4 and 5 digital arrest operations.

- FTC Consent Order against InMobi (2016) — a binding foreign regulatory finding — has never entered India's threat modelling for 10 years.
- Silverpush Technologies is an Indian company in Delhi NCR — never investigated under India's own IT Act Section 43A.
- No SOP addresses: how does the fraudster know the victim is alone at home with a large bank balance? This precision requires real-time data — the adtech SDKs are the only identified source.
- As of April 2026, Aadhaar authentication extended to private entities — expanding the biometric data surface — without investigating whether the adtech layer has been dismantled.

WEAKNESS 3 AI-Amplification Layer — No Model Exists for Generation 5 Operations

Severity: **CRITICAL — EMERGING ONLY**

India's enforcement framework was designed for Generation 1-3 threats. Generation 5 threats — fully AI-automated fraud from offshore servers with no Indian employee, no Indian SIM, no Indian server — operate completely outside the reach of every existing SOP. The apparent decline in digital arrest complaint numbers is not a success indicator — it reflects the threat automating beyond India's detection architecture.

- Voice cloning using stolen audio from RECORD_AUDIO permission — no forensic protocol for AI-generated voice evidence under BNS 2023.
- 80 million KYC records can generate 8 billion+ AI-personalised fraud operations. The model treats 80M as a fixed number; in AI terms it is an exponentially expanding attack surface.
- CNAP and SIM-Binding (2026 rollout) address India-based SIM fraud only. Foreign VoIP — Gen 5 primary channel — bypasses both entirely.
- I4C projects losses of Rs. 1.2 lakh crore in 2026 — confirming Gen 5 scale while complaint numbers decline.

WEAKNESS 4 Jurisdiction Fragmentation — Coordination Failure Officially Acknowledged

Severity: **SERIOUS — PARTIALLY ADDRESSED**

The September 2024 AoB Rules amendment clarified jurisdiction — MHA for crime, MeitY for cybersecurity, DoT for telecom, NSCS for strategic coordination. The Carnegie Endowment for International Peace (September 2025) identified India's organisational measures as its weakest area despite ITU Tier 1 status. Acknowledging fragmentation is not the same as resolving it.

- A Delhi scam linked to Kerala mule accounts and West Bengal SIMs creates three competing jurisdictions with no effective rapid coordination mechanism.
- 459 dedicated cyber police stations — but UP reports backlog in device mirroring. Evidence degrades before analysis.
- MHA defreezing SOP for lien-marked accounts: STILL NOT FINALISED as of January 2026. Victims locked out of their own accounts with no unfreeze procedure.

WEAKNESS 5 Extradition and Impunity Layer — The Structural Immunity of Foreign Principals

Severity: **CRITICAL — POLITICALLY BLOCKED**

The most fundamental weakness in India's threat model is not technical — it is legal-diplomatic. The entire enforcement architecture is designed to operate within Indian jurisdiction. The principals of every major cyber fraud ecosystem operate from outside Indian jurisdiction. The model cannot reach them by design.

- 103 arrested in Operations Hawk and Chakra-II — all Indian nationals. Zero principal architects. This is investigation design, not investigation failure — targeting only what is reachable.
- Section 3(4) Extradition Act 1962 — available since 1993, used zero times against Chinese accused in cyber fraud in 14 years.
- Jeffrey Zhu free since mid-2021 — 5 years. LOC issued after his departure. No confirmed successful Interpol Red Corner Notice processed.
- Pattern of deportation without prosecution — Hyderabad call centre (Dec 2020), Wang Fang Pune (2021) — surrenders India's only criminal leverage for nothing.

[05] SOP ARCHITECTURE — HOW EACH SOP WORKS AND WHERE IT FAILS

India's cyber crime response runs on a layered SOP architecture covering five stages: Detection, Reporting, Freezing, Investigation, and Prosecution. The architecture functions at the first two layers and breaks down from the third layer onward. The following maps each major SOP against its operational parameters, measured effectiveness, and the specific layer of the fraud chain it cannot reach.

SOP 01 — 1930 HELPLINE + e-ZERO FIR (May 2025)

Owner	I4C / MHA
Status	FUNCTIONAL — SCALE OVERWHELMED
How It Works	Citizen calls within 2 hours of fraud. Real-time bank alert. Fund freeze initiated. From May 2025: frauds above Rs. 10L auto-register as Zero FIR removing jurisdictional barrier.
Scale (2025)	88,976 calls/day; 3.24 crore total calls in 2025. One call every second of every day.

Where This SOP Fails:

- Designed for instant fraud, not prolonged coercion. Digital arrest victims held 24-72+ hours cannot call.
- Low-value fraud (below Rs. 10L) — majority of cases — still requires manual FIR. FIR rate dropped to 1.4% in 2025.
- Centre wrote to states in December 2025 asking for 'urgent improvement' in FIR conversion rates.

Data Pipeline Gap: Operates on financial transaction data only. Zero interface with data exfiltration forensics. The data that enabled the fraud is not tracked.

SOP 02 — CFCFRMS FUND FREEZE + MULE AI HUNTER

Owner	I4C + Banks + Payment Aggregators (CFMC)
Status	PARTIAL — DOWNSTREAM ONLY
How It Works	Real-time alert from 1930 to CFMC bank representatives. Freeze within minutes. Mule AI Hunter uses ML to flag suspect accounts. 24 lakh+ mule accounts frozen cumulatively.
Scale	Rs. 8,031 Crore saved cumulatively. 24.67 lakh mule accounts closed in Karnataka alone in 2025.

Where This SOP Fails:

- Mule accounts rotate every 24-72 hours. Funds move 3-5 hops before victim reports. Most money already offshore by call time.
- Karnataka: 70,000+ mule accounts in 2024 — police confirm this is 'first layer only.' Chains extend further.
- Defreezing SOP for lien-marked accounts: NOT FINALISED as of January 2026. Innocent account holders remain frozen with no unfreeze procedure.
- Gen 5 operations use USDT/crypto — entirely outside banking SOP architecture.

Data Pipeline Gap: Mule AI Hunter operates on bank transaction data. Zero access to app-level data streams, SDK traffic, or dark web marketplace activity.

SOP 03 — TELECOM CNAP + SIM-BINDING (2026 Rollout)

Owner	DoT / TRAI
Status	ROLLOUT PHASE — NOT YET LIVE
How It Works	CNAP: incoming calls display verified KYC name — prevents caller impersonation. SIM-Binding: messaging apps deactivate without active physical SIM — prevents burner SIM fraud. Pilot shows 40% fraud drop in test circles.
Scale	CNAP in pilot. Full rollout expected H1 2026. SIM-Binding mandate issued — implementation by Jio/Airtel under testing.

Where This SOP Fails:

- Foreign VoIP calls — Gen 5 primary channel from UAE/Cambodia/China — bypass SIM-Binding entirely. CNAP does not cover international calls.
- Already-exfiltrated data continues to power fraud regardless of CNAP deployment.
- The targeting data (victim's Aadhaar address, real-time bank balance) comes from the data pipeline — which this SOP does not touch.

Data Pipeline Gap: Communication-layer intervention only. Does not address the intelligence layer that makes the fraud call possible.

SOP 04 — PRATIBIMB + JCCT COORDINATION

Owner	I4C / State Law Enforcement Agencies
Status	FUNCTIONAL — DOMESTIC ONLY
How It Works	Pratibimb maps criminal locations and crime infrastructure nationally. 7 JCCTs covering Mewat, Jamtara, Ahmedabad, Hyderabad, Chandigarh, Vishakhapatnam, Guwahati hotspots. 16,840 suspects arrested using Pratibimb in 2025.
Scale	Nationwide deployment. All 7 identified cyber crime hotspot clusters covered.

Where This SOP Fails:

- Pratibimb maps Indian criminal geography. Zero visibility over Chinese server clusters, UAE USDT routing, or Cambodia-based operations.
- JCCT has no international law enforcement cooperation mechanism for cyber fraud principals.
- India-US MoU exists (Jan 2025). India-China: nothing equivalent.

Data Pipeline Gap: All 16,840 arrests are domestic Indian nationals — call centre workers, mule account holders. Not one foreign principal architect in Pratibimb's operational universe.

SOP 05 — CERT-IN INCIDENT RESPONSE

Owner	MeitY / CERT-In
Status	FUNCTIONAL — WRONG TARGET
How It Works	CERT-In handled 29.44 lakh cyber incidents in 2025. Issues vulnerability notes, advisories, early warning alerts. Trusted Telecom Portal bans Chinese-origin telecom hardware.
Scale	1,530 alerts, 390 vulnerability notes, 65 advisories issued in 2025.

Where This SOP Fails:

- CERT-In mandate covers critical infrastructure and network security incidents — not consumer data exfiltration by applications.
- Trusted Telecom Portal covers hardware procurement — does not cover Chinese-owned software SDKs already embedded in citizen devices.
- No CERT-In advisory has ever addressed InMobi, Silverpush, or SDK-based data exfiltration as a national security threat vector.

Data Pipeline Gap: CERT-In monitors network-level and infrastructure threats. Consumer-application data pipeline — the actual mechanism of the 80M breach — is not within its operational mandate.

5.1 SOP Coverage Matrix — The Seven Stages of the Fraud Chain

STAGE	WHAT HAPPENS	SOP COVERAGE	UNCOVERED — THE ACCOUNTABILITY GAP
Stage 1 App Install	Victim installs app. Grants permissions bundle including	Minimal. Google Play policies. No MeitY APK audit mandate.	No SOP mandates minimum-necessary permissions audit before app listing. SDK

	contacts, SMS, GPS, microphone, camera.		content of apps not audited. Sideloaded APKs completely unregulated.
Stage 2 Data Harvest	App harvests complete digital identity. Uploads to C2 server every 24-72 hours.	IT Act S.43A + IT Rules 2011 (unenforced). DPDPA (not operative till May 2027).	No real-time monitoring of C2 uploads. No SDK traffic analysis SOP. No mandatory data collection disclosure register.
Stage 3 KYC Merger	Shell NBFC collects Aadhaar + PAN + face biometric + bank account. Merges with device data.	RBI Digital Lending Guidelines 2022 (prospective only).	No retrospective forensic audit of NBFC data storage. No SOP for historical KYC data destruction.
Stage 4 Foreign DB	Complete identity profile stored on foreign-controlled servers in China / UAE.	**NONE.**	Zero diplomatic, legal, or technical SOP reaches foreign servers. No MLAT. No extradition request. Absolute jurisdictional void.
Stage 5 Dark Web	80M+ KYC bundles sold on dark web. Buyers include fraud operations globally.	CERT-In monitors dark web (limited). No enforcement jurisdiction.	No SOP for taking down dark web listings of Indian citizen data. No victim notification protocol.
Stage 6 Fraud Call	Fraudster calls with victim's exact address, balance, family details. Prolonged coercion.	1930 Helpline (requires victim escape). CNAP pilot (domestic SIMs only). PM awareness Oct 2024.	How fraudster has REAL-TIME targeting data — never investigated. Adtech layer never modelled. Root cause of targeting precision: absent from all SOPs.
Stage 7 Money Move	Victim transfers funds. Move through mule chain, crypto, hawala to offshore accounts.	CFCFRMS + 1930 + Mule AI Hunter + Bank freeze. Most functional SOP layer.	Recovery below 10% (Karnataka 2025). Crypto/USDT flows outside all SOP architecture.

[06] ENFORCEMENT GAPS — DOCUMENTED OFFICIAL RECORD OF WHAT DID NOT HAPPEN

The following documented gaps constitute the evidentiary foundation of this petition's accountability argument. Each gap is established from official government documents, Parliamentary records, or verified published research — not from private assertions by the petitioner. The gaps span from 2012 to April 2026.

GAP 1 | 2016 — April 2026 (10 years)

InMobi / Silverpush — Zero Indian Regulatory Action in 10 Years

The US Federal Trade Commission issued a Consent Order against InMobi (2016) and Warning Letters against Silverpush Technologies (2016) — both publicly available documents establishing illegal SDK-based surveillance of users without consent. MeitY received constructive notice from June 2016. As of April 2026: not one inquiry, show-cause notice, or penalty proceeding has been initiated against either entity under IT Act Section 43A or DPDPA. Silverpush Technologies is an Indian company registered in Delhi NCR — India has had jurisdiction for 10 years. The inaction is documented and verifiable by the absence of any official record of proceedings on MeitY's own website.

GAP 2 | 2021 — April 2026 (5 years)

Jeffrey Zhu / Zhu Wei — 5 Years of Impunity; Section 3(4) Never Invoked

Jeffrey Zhu (a.k.a. Zhu Wei) departed India in mid-2021 before the Look Out Circular was issued — a documented investigative failure. Section 3(4) of the Extradition Act 1962 provides for extradition without a bilateral treaty where the offence is covered by UNCAC or other multilateral convention. Both India and China are parties to UNCAC since 2003 and 2006 respectively. In 5 years, the government has filed zero extradition requests under this provision against Zhu Wei or any other Chinese national in the digital fraud ecosystem. The master database of 80 million Indian citizens' biometric data remains under his effective control. The non-filing is verifiable by the absence of any public record of extradition request filing in the Ministry of External Affairs.

GAP 3 | 2021 — April 2026 (5 years)

80 Million Victims — Zero Breach Notification Issued to Any of Them

CloudSEK documented 80 million+ Indian KYC records in active dark web circulation in August 2021. The report was publicly available and verified through crossmatching by independent researchers. As of April 2026 — five years later — not one of the 80 million affected citizens has received any notification from any government body that their Aadhaar number, PAN card number, face biometric, bank account details, and residential address is in criminal hands and being actively weaponised against them. The DPDPA breach notification provisions will only become operative in May 2027. The government has the constitutional power to notify under Article 21 regardless of the statutory timeline — and has not done so.

GAP 4 | 2020 — 2024

Pattern of Deportation Without Prosecution — Surrendering Criminal Jurisdiction

Six Chinese nationals arrested at a Hyderabad call centre in December 2020 — deported without criminal prosecution in India. Wang Fang arrested in Pune (2021) — deported without prosecution. This pattern across every Chinese national physically arrested in India in this ecosystem represents a deliberate choice to surrender India's only available criminal jurisdiction in exchange for no documented diplomatic benefit. Once deported, India has zero remaining legal leverage over these individuals. The deportation records are verifiable from press releases of the agencies concerned.

GAP 5 | 2023 — April 2026

DPDPA — 27 Months to Phase I; Substantive Enforcement 45 Months After Enactment

The DPDPA was enacted on 11 August 2023. The DPDP Rules were notified 27 months later on 13 November 2025. The Data Protection Board establishment provisions came into force on 13 November 2025, but Board members have not yet been appointed as of April 2026. All substantive provisions — consent, breach notification, security obligations,

and penalties — will only become operative on 13 May 2027, 45 months after enactment. Parliament enacted this law in response to the Puttaswamy judgment (2017) and the very data breach this petition concerns. The 45-month implementation gap is itself a constitutional accountability question.

GAP 6 | Ongoing

FIR Conversion Rate: 1 in 45 Complaints — Centre Itself Acknowledges Crisis

As of December 31, 2025, the national average FIR conversion rate for cyber crime complaints was 2.22%. The provisional 2025 figure is 1.4% — meaning only 1 in 71 complaints became an FIR in 2025. The Centre has written to all states asking for urgent improvement in FIR conversion rates (Source: The420.in, April 2026, citing official Centre communication). Combined with the conviction rate of 2.3% (NCRB 2023), the combined probability that a cyber crime complaint results in conviction is approximately 1 in 2,000. India's criminal justice system is not a deterrent. It is not even a risk factor for professional transnational cyber fraudsters.

[07] COURT-READY FINDINGS — UPDATED ARGUMENTS FOR SUBMISSION

The following findings are stated in terms suitable for oral argument and written submissions before the Supreme Court. Each finding is supported entirely by official government data or official institutional analysis. None relies on private research not corroborated by official sources.

FINDING 1 — The DPDPA Argument Must Be Updated — A Stronger Version Is Available

The petition's original argument that the Data Protection Board 'was never constituted' must be replaced. The updated argument: the DPDP Rules were notified on 13 November 2025 but substantive enforcement — consent, breach notification, penalties — will only become operative on 13 May 2027, forty-five months after enactment. The 80 million citizens whose data was stolen in 2020-2022 will have waited seven years for statutory breach notification protection. This Court under Article 32 read with Article 142 can direct immediate breach notification as a constitutional interim direction, independent of the statutory phased timeline designed for prospective compliance, not historical breach victims.

FINDING 2 — Every Government SOP Operates Downstream of the Data Theft — Proven by Official Data

CNAP and SIM-Binding address call spoofing. The 1930 Helpline and CFCFRMS address money movement. Mule AI Hunter addresses account patterns. Pratibimb addresses domestic criminal geography. Not one SOP has the data pipeline — Stages 1 through 5 of the fraud chain — as its operational target. This is established entirely from official I4C, MHA, DoT, and RBI publications. The absence of a data-pipeline SOP is the government's own negative record — verifiable by searching official press releases, Parliamentary replies, and agency websites for any reference to SDK data traffic investigation, adtech layer audit, or C2 server forensics. No such reference exists.

FINDING 3 — The FIR Conversion Rate Crisis — Government's Own Communication to States as Evidence

The Centre wrote to all state governments in late 2025 acknowledging that the FIR conversion rate is a crisis requiring urgent improvement. This official Centre communication is the single strongest new piece of evidence for the petition's argument that ordinary criminal justice has structurally failed. It is not a private allegation — it is the government writing to itself acknowledging the failure. Combined with the 2.3% conviction rate (NCRB 2023) and the 1.4% provisional FIR rate in 2025, the submission is: India's criminal justice framework is not operationally capable of deterring transnational cyber crime — and the government's own communications confirm this.

FINDING 4 — Carnegie Endowment Analysis Confirms the Petition's Architecture Argument

The Carnegie Endowment for International Peace (September 2025) analysed India's cybersecurity administration structure following the AoB Rules amendment. Its finding: India's legal frameworks and technical capabilities are strong; its organisational measures are the weakest element despite ITU Tier 1 Cybersecurity Index ranking. This is the identical structural argument made in this petition — that the failure is not in the absence of laws or infrastructure, but in the organisational decision to investigate money rather than data, to arrest workers rather than architects, to deport rather than prosecute. The government's own international peer review confirms the petitioner's diagnosis.

FINDING 5 — The Apparent Decline in Digital Arrest Complaints Is an Aggravating Indicator, Not a Success

Digital arrest complaints: 22,479 cases in 2024 with Rs. 2,500 crore loss. January to November 2025: 13,599 cases with Rs. 2,038 crore loss. The government may present this as enforcement success. It is not. Generation 5 cyber fraud operations are fully AI-automated — no Indian employee, no Indian SIM, no Indian server. Fewer complaints reflect the fraud automating beyond India's detection architecture, not retreating. I4C's own projection of Rs. 1.2 lakh crore in losses for 2026 — announced simultaneously with the complaint decline — confirms that automation is accelerating, not retreating. A declining complaint count with an accelerating loss projection is not a success story. It is a warning that the threat has permanently outpaced every existing SOP.

FINDING 6 — Section 3(4) Extradition Act — 14 Years of Non-Invocation is a Constitutional Accountability Question

The Solicitor General will argue that extradition strategy is an Executive prerogative. That argument does not answer the constitutional question this petition raises. Parliament enacted Section 3(4) of the Extradition Act 1962 specifically to enable extradition without a bilateral treaty. Parliament enacted UNCAC obligations that India accepted in 2011. The question is not whether the Executive should extradite Zhu Wei. The question is whether the Executive is constitutionally obligated — under Article 14 read with Article 21 — to explain before this Court why a statutory tool created by Parliament for exactly this situation was not invoked for 14 years against any Chinese accused in any cyber fraud case affecting 80 million Indian citizens. The explanation may exist. Under the Constitution, it must be given — and under oath.

[APP. A] SOURCES AND OFFICIAL REFERENCES

All data cited in this research dossier is sourced from official government publications, Parliamentary records, or peer-reviewed institutional analysis. The following is a complete reference list categorised by source type.

MINISTRY OF HOME AFFAIRS / I4C — OFFICIAL GOVERNMENT SOURCES

- PIB Press Release PRID:2205201 (17 Dec 2025) — Cyber Security and Financial Fraud Combat — I4C statistics on SIM blocking, IMEI blocking, CFCFRMS savings.
- Lok Sabha Unstarred Question No. 452 (02.12.2025) — MHA Parliamentary Reply — State/UT wise cyber crime data, training programs, operational statistics.
- Lok Sabha Starred Question No. 204 (10.12.2024) — MHA Parliamentary Reply — I4C infrastructure, JCCT workshops, Pratibimb module, forensic lab details.
- PIB Press Release PRID:2198253 (03.12.2025) — Cyber Crime Cases and Forensic Capabilities — NCFL Assam, forensic lab coverage.
- PIB Press Release PRID:2112244 (2025) — Steps to Curb Cyber Crime — SIM/IMEI blocking data, CFCFRMS figures.
- MHA Lok Sabha Reply PRID:2003158 (06.02.2024) — Cases of Cyber Frauds — Official complaint/FIR data.
- I4C Website (i4c.mha.gov.in/about.aspx) — Scheme structure, 7 components, objectives.

NCRB OFFICIAL PUBLICATIONS

- Crime in India 2022 (NCRB) — State/UT wise cyber crime cases registered, chargesheeted, convicted.
- Crime in India 2023 (NCRB) — 86,420 cyber crime FIRs, 31% increase over 2022, 2.3% conviction rate data.
- NCRB Data: 2.3% conviction rate for cyber crime cases (2023, cited in India Data Map analysis).

DPDPA — OFFICIAL LEGAL SOURCES

- Digital Personal Data Protection Act, 2023 (Parliament of India, 11 August 2023).
- Digital Personal Data Protection Rules, 2025 (MeitY notification, 13 November 2025) — Phased implementation timeline.
- MeitY Official Notification (13 November 2025) — Phase I provisions brought into force.

INSTITUTIONAL AND PEER-REVIEWED ANALYSIS

- Carnegie Endowment for International Peace (September 2025) — 'Mapping India's Cybersecurity Administration in 2025' — AoB Rules analysis, organisational weakness assessment.
- Hogan Lovells (2025) — 'India's Digital Personal Data Protection Act 2023 Brought Into Force' — Phased implementation legal analysis.
- IAPP (International Association of Privacy Professionals, Jan 2026) — 'Top 10 Operational Impacts of India's DPDPA.'
- EY India (April 2026) — DPDPA compliance guidance, 72-hour reporting and board oversight analysis.

VERIFIED JOURNALISM AND DATA PLATFORMS

- The420.in (21 April 2026) — 'Centre Flags Wide Gap Between Cybercrime Complaints, Only 1-3% Become FIRs' — FIR conversion rate data citing official Centre communication to states.
- The420.in (5 January 2026) — 'Banks Are Responding Faster But Why Mule Accounts Keep Increasing' — Karnataka police data, defreezing SOP non-finalisation.
- The420.in (27 December 2025) — 'Top 10 Most Highlighted Cyber Crime Cases and Trends in India in 2025' — I4C projections, Rs. 1.2 lakh crore 2026 projection.
- The420.in (29 December 2025) — 'India's 2026 Telecom Revolution: CNAP and SIM-Binding Rules' — CNAP/SIM-Binding technical details.
- Cyber Mithra (30 December 2025) — '2025: The Year of Cyber Security' — 2024/2025 complaint comparison.
- Insights on India (21 February 2026) — 'Cybercrime in India 2025' — 28.15 lakh complaints, forensic talent gap, jurisdictional hurdles.
- BOOM Live (6 October 2025) — 'NCRB Data on Cyber Crimes Dated, Not Indicative of True Picture' — Expert analysis of NCRB data limitations.

- Drishti IAS (28 January 2026) — 'Strengthening India's Cyber Security Architecture' — CERT-In 2025 statistics, Sanchar Saathi data.

STATEMENT OF SOURCES: This research dossier relies exclusively on official government documents, Parliamentary records, peer-reviewed institutional analysis, and verified journalism from recognised cyber crime reporting platforms. No unverified private research has been cited. All figures attributed to government sources reflect the government's own published data.

Prepared by: Nitish Kumar, Petitioner-in-Person | April 2026 | Supreme Court of India | CONFIDENTIAL