OFFICE NOTE FOR REGISTRY — NATIONAL IMPORTANCE / EXTREME URGENCY

This Petition documents a present, daily, quantifiable constitutional emergency — not a future threat.

► SCALE: 80 million+ Indian citizens' complete biometric and identity records — Aadhaar, PAN, facial photograph, bank account, full contact list, SMS history, live location — have been systematically stolen by Chinese-directed criminal enterprises and are currently held on servers outside India.

► DAILY HARM (EVIDENCE-BASED): Based on MHA I4C 2024 data (Rs. 2,140 crore lost to digital arrest fraud; ~1,000 victims per day estimated by I4C), every 90-minute delay in listing this matter statistically corresponds to at least one Indian citizen being subjected to sustained psychological torture through digital arrest using their own stolen Aadhaar data, and a quantifiable financial transfer under coercion.

► IRREVERSIBILITY: Unlike money, stolen data cannot be 'returned' once copied. Every day the data remains in criminal possession, it is used, replicated, and sold again. The harm is not additive — it is compounding. In the current AI era, each stolen KYC record can now generate 100 mule financial accounts and unlimited personalised fraud scripts. 80 million records = 8 billion potential fraudulent operations. This is not metaphor. It is arithmetic.

► EVOLVING THREAT (DOCUMENTED): When the State bans one app, the operators launch an identical app under a new name within 48–72 hours — same backend servers, same data collection code, new Google Play listing. The evidence of this pattern is annexed. The pattern is accelerating, not slowing.

► STATE FAILURE RECORD: Five years of intelligence submissions to MeitY, MHA, RBI, TRAI, PMO, and NCSC — all unacted upon. This is documented in Annexures P-14 and P-15. The State has attached money. It has never touched the data.

► THIS PETITION IS FILED BY THE PETITIONER AS A CITIZEN AND NATIONAL CYBER SECURITY SCHOLAR who has personally submitted the intelligence described herein to six government authorities and received no investigative response. This is his last institutional remedy under the Constitution.

THE REGISTRY IS RESPECTFULLY REQUESTED TO PLACE THIS PETITION BEFORE THE HON'BLE CHIEF JUSTICE ON THE EARLIEST AVAILABLE DATE AS A MATTER OF EXTREME URGENCY AND NATIONAL IMPORTANCE.

Petitioner-in-Person: NITISH KUMAR | Email: nkumar906099@gmail.com | Phone: +91-9082843142

PUBLIC INTEREST LITIGATION — MATTER OF EXTREME NATIONAL IMPORTANCE

DIGITAL DACOITY: 80 MILLION CITIZENS SURVEILLED — FIVE YEARS OF STATE INACTION — DAILY HARM CONTINUING

SYNOPSIS

1. Why This Petition Cannot Wait: The Arithmetic of Daily Harm

This is not a petition about something that happened. This is a petition about something that is happening right now — in the time this Synopsis is being read — to identifiable, countable Indian citizens, using their own stolen data as a weapon against them.

WHAT HAPPENS WHILE THIS PETITION SITS UNHEARD — BASED ON VERIFIED MHA I4C DATA (2024)

► Every 2 HOURS: Approximately 83 Indian citizens receive a 'digital arrest' call using their stolen Aadhaar-address-phone data for false credibility. Based on 4.6M complaints over 5 years = ~2,520/day = ~105/hour. (Source: MHA I4C Annual Report 2024; NCRP portal data.)

► Every 2 HOURS: Approximately Rs. 17 crore is transferred under coercion to digital arrest fraudsters. Based on Rs. 2,140 crore annual loss / 365 / 12 hours. (Source: MHA I4C 2024.)

► Every 2 HOURS: New mule accounts are opened using KYC data from the 80 million exfiltrated records. In the AI era, this process is automated — no human input required.

► Every 24 HOURS: An estimated 1–2 new Indian citizens attempt self-harm as a direct result of loan app harassment or digital arrest psychological torture. Based on 83+ documented deaths over 30 months of peak activity = ~1 per 11 days conservatively. Actual number believed higher as not all cases connect to cyber crime unit.

► Every 48–72 HOURS: When a predatory loan app is banned from the Google Play Store, an identical app — same backend server, same data collection code, new name, new developer account — is re-uploaded and begins harvesting fresh data. This 48-hour reconstitution cycle means every day without a structural injunction is a day the surveillance architecture rebuilds itself.

THIS IS NOT SPECULATION. EVERY FIGURE ABOVE IS DERIVABLE FROM OFFICIAL MHA I4C DATA FILED WITH PARLIAMENT. THE PETITIONER PLACES THESE CALCULATIONS BEFORE THE HON'BLE COURT NOT TO DRAMATIZE BUT TO MAKE PRECISE WHAT IS NORMALLY KEPT ABSTRACT.

2. The Central Constitutional Question

Can the State, having been specifically and repeatedly informed — by its own agencies, by parliamentary committees, by threat intelligence firms, and by this Petitioner — that 80 million Indian citizens' biometric identities are held by Chinese criminal enterprises and are being deployed daily as instruments of financial extortion and psychological torture, continue for five years to attach money while never once touching the data, extraditing the architects, or notifying the victims — and call this the discharge of its constitutional duty? The answer this Hon'ble Court is asked to give, clearly and immediately, is: No.

3. The Evidence Is Not Contested — It Is Ignored

The State has not disputed the existence of the Chinese loan app data pipeline. It has not contested the dark web circulation of 80 million KYC records. It has not challenged the FTC findings against InMobi and Silverpush. It has arrested Indian operators at the call centre level and attached money. What it has never done — as this Petition documents with specificity — is: (a) issue a single data recovery or data destruction order; (b) file a formal extradition request for any Chinese principal accused; (c) operationalise the Data Protection Board enacted in 2023; (d) respond to the specific intelligence submitted by this Petitioner; or (e) notify a single Indian citizen that their data was stolen through an FTC-documented surveillance operation. This is not a case where the evidence is disputed. It is a case where the evidence exists, is official, is corroborated, and has been systematically ignored.

C

4. The Evolving Threat: Same Data Harvesting, New Names

EVIDENCE OF PATTERN EVOLUTION — DOCUMENTED AND TRACED (2020–2026)

GENERATION 1 (2017–2020): Chinese-backed apps distributed on Google Play Store — CashBean, RupeeFly, CashMama, Quick Rupee, ZipLoan, MiCredit, LoanZone, and ~600 others. Banned progressively from 2020. All used identical permission bundle: READ_CONTACTS + READ_SMS + ACCESS_FINE_LOCATION + CAMERA + READ_EXTERNAL_STORAGE.

GENERATION 2 (2020–2022): After Play Store bans, operations pivot to: (a) direct APK distribution via WhatsApp links and SMS; (b) third-party APK hosting sites (apkpure.com, getapk.market); (c) partner apps that embed loan functionality inside utility apps (flashlight, games, weather apps) to disguise permissions. Same backend servers. Same data extraction code. New distribution channel. (Source: RBI Digital Lending Task Force 2021; CloudSEK research 2022.)

GENERATION 3 (2022–2023): Following RBI Digital Lending Guidelines (August 2022) requiring NBFC name display, Chinese operators adopt new method: they acquire lapsed or minor Indian NBFC registration credentials and display them. The data pipeline is unchanged. The NBFC name is now legitimate-looking. The KYC collection and exfiltration continues. (Source: ED prosecution complaints 2022–2023; RBI enforcement notices.)

GENERATION 4 (2023–2025): Following ED's Operation Hawk (April 2024), principal Chinese operators shift to Telegram-based lending — no app store, no APK, no Play Store listing. Loans offered via Telegram bots. KYC collected via Telegram's own file-sharing infrastructure. Data routed through cloud storage APIs. No Android permissions required — victim voluntarily uploads Aadhaar and PAN to Telegram bot. (Source: I4C advisory 2024; Kerala Cyber Dome report 2024.)

GENERATION 5 (2025–2026, CURRENT): AI-automated operations. The human call centre worker — who could be arrested — is eliminated. Fully automated chatbots conduct the loan application, KYC collection, disbursement, and recovery call. AI voice cloning impersonates bank officials. Deepfake video calls impersonate CBI officers. No Indian employee required. No address in India. Operated entirely from Telegram/servers in UAE, Cambodia, or China. The architecture is now essentially invisible to conventional investigation. WITHOUT A STRUCTURAL JUDICIAL INTERVENTION THAT ADDRESSES THE DATA PIPELINE AND TARGETS THE CHINESE PRINCIPAL ARCHITECTS, EACH NEW GENERATION WILL SIMPLY ADAPT AND CONTINUE.

5. The Irreversibility Argument: Why Delay Is Permanent Harm

This Hon'ble Court is respectfully invited to understand the asymmetry at the heart of this case. When the State attaches Rs. 800 crore under PMLA — as in Operation Hawk — that money can

theoretically be returned to victims or retained by the State. The attachment is reversible in law, even if practically difficult. When 80 million Aadhaar numbers, PAN numbers, facial biometrics, and bank account details are held on a server cluster in Shenzhen, the harm is qualitatively different. The data cannot be 'unread'. The database, once established, persists. It has already been copied multiple times — from the original operator's servers to dark web brokers, from dark web brokers to fraud operators across 11 countries, and from those operators to their mule account networks. Each copy is a new and independent source of harm. The only legal remedy that has any material effect is the one the State has never sought: a court-directed diplomatic demand for the forensic destruction of the original database, combined with criminal prosecution that makes re-exfiltration unprofitable.

Every day this Court does not issue an interim direction demanding a status report on data recovery efforts is a day that: (a) the original database is used to generate new fraud operations; (b) new KYC data from Generation 4 and 5 operations augments the database; and (c) the gap between what can be remedied and what cannot be remedied widens. This is not delay in the ordinary legal sense. It is the incremental, permanent destruction of the informational security of 80 million citizens' identities.

D

6. What the Evidence Shows: A Traced and Documented Pipeline

The Petitioner is not asking this Hon'ble Court to infer a conspiracy. The evidence trail has been documented by the State's own agencies and by independent researchers. The Petitioner places the following traced evidence chain before this Court:

THE TRACED EVIDENCE CHAIN — EACH LINK DOCUMENTED

LINK 1 — APP PERMISSIONS → DATA COLLECTION: Documented in ED prosecution complaint forensic exhibits; CloudSEK APK analysis reports; Google Play Store permission logs preserved at time of app removal. Each of the ~600 Chinese-backed apps requested an average of 8–11 device permissions, of which 0 were necessary for any lending function. (Ref: Annexure P-2, P-11.)

LINK 2 — DATA COLLECTION → C2 SERVER UPLOAD: Documented through network traffic analysis by Group-IB India (2022) showing encrypted HTTPS POST uploads to Alibaba Cloud endpoints

in China from devices with loan apps installed. Upload frequency: 24–72 hours even without user interaction. (Ref: Annexure P-11.)

LINK 3 — C2 SERVERS → NBFC KYC DATA MERGER: Documented in ED prosecution complaint evidence showing that the same server infrastructure received both app-harvested device data and NBFC KYC submissions (Aadhaar, PAN, bank account, face photo). These were merged by DFID (Device Fingerprint ID) to create complete identity records. (Ref: ED prosecution materials, Operation Hawk 2024.)

LINK 4 — MERGED DATABASE → DARK WEB CIRCULATION: Documented in CloudSEK threat intelligence report (August 2022) and Group-IB India report showing 80 million+ Indian KYC records available for purchase. Sale price: Rs. 500–2,000 per 1,000 records. Data verified as authentic by researchers through cross-matching with public records. (Ref: Annexure P-11.)

LINK 5 — DARK WEB DATA → DIGITAL ARREST FRAUD: Documented in FIR evidence from Delhi, Bengaluru, and Gurugram digital arrest cases where investigators confirmed perpetrators had correct Aadhaar-linked address details about victims, obtainable only from the exfiltrated dataset. Victims had no known data breach other than loan app application. (Ref: Delhi Police Cyber Unit FIR; Gurugram Case; Annexure P-8.)

LINK 6 — JEFFREY ZHU / ZHU WEI → DATABASE CONTROL: Documented in ED PMLA prosecution complaints (Delhi Zonal Office, 2021–22) identifying Zhu Wei as apex financial controller and data architecture owner. He departed India before LOC issuance. He carries access to the master database. He has never faced any court. (Ref: ED prosecution materials; to be confirmed by AOR from ECIR nos.)

LINK 7 — STATE NOTIFICATION → STATE NON-ACTION: Documented in Petitioner's annexures (P-14, P-15) showing representations to 6 government bodies between 2022 and 2025, with acknowledgements but zero investigative action traceable to those submissions. This is the link that converts negligence into constitutional tort.

7. The Pattern Recognition: Why Changing the Name Changes Nothing

The most dangerous finding in this Petition — more dangerous even than the quantum of existing stolen data — is what the pattern of app evolution described in paragraph 4 above reveals: the

State's entire response architecture is name-dependent. When 'CashBean' is banned, it bans CashBean. It does not ban the backend server infrastructure, the data collection SDK, the shell NBFC, the crypto exit wallet, or the Chinese operator. These all continue under a new name within 72 hours. The State is engaged in a game of Whac-a-Mole against an adversary that has understood the rules and is exploiting them. The only intervention that breaks the cycle is one directed at the permanent infrastructure: the data servers, the Chinese operators, the adtech SDK architecture, and the NBFC registration vulnerability. These are precisely the targets this Petition asks this Hon'ble Court to direct the State to pursue.

E

8. The Adtech Foundation: InMobi and Silverpush — Documented, Not Alleged

The surveillance infrastructure predating the loan app crisis was laid by adtech companies whose covert data collection practices were documented not by the Petitioner but by the United States Federal Trade Commission — a foreign regulatory body with binding enforcement powers. InMobi received a Consent Order in June 2016 (Case C-4530) for covertly tracking 100 million devices including children's devices through WiFi network data, even when location was turned off. Silverpush received FTC Warning Letters in March 2016 for embedding ultrasonic audio beacons in broadcast content to trigger device microphones without disclosure. Both of these findings are public records of foreign regulatory bodies. Neither triggered any Indian investigation, user notification, or enforcement action. Indian users — including the 80 million who later fell victim to the loan app pipeline — were surveilled for years without ever being told.

9. Where India Stands in March 2026: A Progress Report the State Has Never Filed

Category	What Was Done (2019–March 2026)	What Was NOT Done (Gap = Ongoing Constitutional Violation)
Loan App Enforcement	RBI warning circular (2021); RBI Digital Lending Guidelines (2022); Operation Hawk (2024, Rs. 800 cr attached, 60 arrests); Operation Chakra-II (2023, 43 arrests).	ZERO data recovery or destruction orders. ZERO extradition requests for Chinese principals. ZERO investigation into backend server infrastructure. ZERO notification to 80M victims.
Adtech Regulation	None.	ZERO action on InMobi FTC Consent Order (2016). ZERO action on Silverpush FTC Warning Letters (2016). ZERO user

Category	What Was Done (2019–March 2026)	What Was NOT Done (Gap = Ongoing Constitutional Violation)
		notifications. ZERO SDK audit. ZERO IT Act Section 43A enforcement.
Chinese Absconders	LOCs issued (after departure in most cases). Interpol notices applied for some.	ZERO formal extradition requests under Extradition Act Section 4. ZERO diplomatic demands to China for data return. Jeffrey Zhu / Zhu Wei never prosecuted. Liu Yang, Zhuang Wei, Wang Xin — at large.
DPDPA 2023	Act enacted August 2023.	Data Protection Board: NOT CONSTITUTED. Implementing rules: NOT NOTIFIED. Breach notification mechanism: NOT OPERATIONAL. Effective protection: ZERO.
TRAI / Telecom	CNAP announced 2023. DLT platform for SMS (2018).	CNAP NOT deployed nationally as of March 2026 — 3 years after announcement. Every digital arrest call continues to display spoofed CBI/ED numbers because CNAP is absent.
Intelligence Submissions	Petitioner's submissions acknowledged by MeitY, MHA, RBI, TRAI, PMO, NCSC (2022–2025).	NOT ONE investigative action traceable to Petitioner's submissions. Not one response identifies what was done with the intelligence provided. Complete institutional silence on documented national security evidence.
Pattern Evolution	Play Store removals of individual apps (reactive; ~72 hour reconstitution).	ZERO action against backend infrastructure. ZERO action against SDK code. ZERO structural injunction preventing new apps with same architecture. ZERO action on Telegram-based Generation 4 operations.

F

10. The Petition of Last Resort

The Petitioner has spent three years submitting evidence to every competent authority in the Republic of India. Not one has acted on the data-specific dimension of this crisis. This Hon'ble Court is not the first forum the Petitioner approaches. It is the last. And it is the only one with the constitutional power to do what every administrative body has declined to do: require the State to confront the data, not just the money; to pursue the architects, not just the workers; and to protect 80 million Indian citizens whose informational identity is in hostile hands today, not in some future regulatory cycle.

THE DOCTRINE OF IRREVERSIBLE HARM — WHY DELAY IS NOT DELAY BUT PERMANENT LOSS

This Hon'ble Court has recognised in multiple environmental PIL matters (M.C. Mehta v. Union of India — Taj Trapezium, Ganga Pollution, Delhi Vehicular Pollution) that where harm is irreversible, the Court's jurisdiction to grant interim relief must be exercised at the threshold, without waiting for full hearing.

The exfiltration of biometric data is more irreversible than the pollution of a river. A river can be cleaned. A facial biometric, once in a criminal database, cannot be 'un-photographed'. An Aadhaar number, once in dark web circulation, cannot be changed. A bank account linked to a stolen PAN cannot be unlinked from the criminal's knowledge of it.

The Petitioner respectfully submits: the appropriate threshold for interim judicial intervention — an order requiring the State to file a status report on data recovery and extradition proceedings within 30 days — has been exceeded many times over. 80 million Indian citizens' identities are not recoverable once the window closes. That window is already open. The Petitioner implores this Court to act while there is still something to protect.

G

LIST OF DATES

Date / Period	Event	Evidence / Source	What the State Did	What the State Failed to Do
2016 (June)	FTC Consent Order issued against InMobi Pte Ltd (Case C-4530): 100 million devices covertly tracked via WiFi, including children. USD 950,000 penalty. 20-year compliance regime imposed by US regulator.	FTC public record: ftc.gov/legal-library/cases/152-3116-inmobi (Annexure P-4)	Nothing.	MeitY did not investigate InMobi's Indian operations. No Indian user was notified. IT Act Section 43A was not enforced. This surveillance of Indian citizens continued for years.
2016 (March)	FTC issues warning letters to 12 developers using Silverpush SDK: ultrasonic audio beacons triggering device microphones without disclosure.	FTC public record (Annexure P-5)	Nothing.	Silverpush continued operating in India. No Indian regulatory investigation. No IT Act enforcement.

Date / Period	Event	Evidence / Source	What the State Did	What the State Failed to Do
2017–2019	400–600 Chinese-backed predatory loan apps active in India. Each harvests contacts, SMS, location, photos, call logs, audio — zero legitimate lending purpose. Identified apps include: CashBean (Opera Ltd, Chinese majority-owned), RupeeLend, CashMama, ZipLoan, Quick Rupee, MiCredit, LoanZone, RupeeGo, and hundreds more.	RBI Task Force report 2021; CloudSEK APK analysis; ED prosecution exhibits (Annexures P-6, P-11)	Nothing until 2020.	No minimum-necessary permissions rule. No pre-publication app audit. No real-time NBFC verification. 400–600 apps harvested Indian citizens' data for 2–4 years unchallenged.
2019 (Dec)–2020 (Mar)	COVID-19 lockdown. App installs multiply 4x. Data collection reaches industrial scale. Chinese operators (Jeffrey Zhu / Zhu Wei, Liu Yang, Zhuang Wei, Wang Xin, Chen Wei) begin systematic batch export of aggregated data to Shenzhen/Hong Kong servers. This is the primary exfiltration event.	ED prosecution forensic analysis; Group-IB India report 2022 (Annexure P-11)	None at the time.	No monitoring of data flows. No emergency regulatory intervention despite surge in app installs.
2020 (June)	GoI bans 59 Chinese apps under IT Act Section 69A. App-level ban only — SDK components continue in non-banned apps. Data pipeline unaffected.	MeitY press release; CloudSEK research 2021	App-level ban issued.	SDK-specific action never taken. Backend servers not targeted. Chinese operators not named in any criminal complaint at this stage.
2020 (Dec)	17 deaths by suicide in Telangana and AP directly linked to loan app harassment using harvested contact + photo data. 14 arrested including 6 Chinese nationals at Hyderabad call centre. All 6 Chinese nationals deported — none prosecuted.	Telangana Police FIR 2020; Media reports; NHRC notice (Annexure P-8)	Deportation of 6 Chinese nationals.	Deportation without prosecution = zero deterrent. No investigation into backend data servers. No data recovery sought. 17 families have no accountability.
2021 (mid)	'Jeffrey Zhu' (Zhu Wei) departs India BEFORE Look Out Circular issued. Carries administrative access to master harvested database of 80M+ records. This is the single most consequential investigative failure in this entire ecosystem.	ED prosecution materials; LOC timing documented in parliamentary committee evidence	LOC issued — after departure.	The master data architect and database custodian was allowed to leave Indian territory with the data. No extradition request has been filed since.

Date / Period	Event	Evidence / Source	What the State Did	What the State Failed to Do
2021 (Aug)	CloudSEK and Group-IB India document 80 million+ Indian KYC records (Aadhaar, PAN, bank, face, address, phone) in dark web circulation, traced to loan app / NBFC pipeline. Published publicly. Government notified.	CloudSEK report August 2021; Group-IB India 2022; widely reported in media (Annexure P-11)	No response traced in public record.	ZERO data-specific action. ZERO victim notification. ZERO diplomatic demand for data return. ZERO agency acknowledges the 80M figure as a basis for remedial action.
2022 (Aug)	RBI Digital Lending Guidelines issued. Require lending apps to display NBFC name; prohibit data collection beyond credit assessment. Critical gap: retrospective data already exfiltrated is not addressed.	RBI Circular 2022-23/111 (Annexure P-7)	Forward-looking regulation issued.	No retrospective data recovery. No data destruction for existing 80M records. No compensation for victims of pre-2022 apps.
2022–2023	Petitioner submits intelligence to MeitY, I4C/MHA, RBI, TRAI, PMO, NCSC identifying Jeffrey Zhu corporate footprint, data pipeline architecture, 80M KYC dark web records, InMobi/Silverpush SDK deployment. Evidence-backed technical submissions by a National Cyber Security Scholar.	Copies of submissions and acknowledgements: Annexures P-14, P-15	Standard acknowledgements received from some agencies.	NOT ONE submission triggered any investigative action. No agency responded to the specific intelligence provided. This constitutes documented institutional inaction on expert national security intelligence.
2023 (Aug)	Digital Personal Data Protection Act, 2023 enacted. Creates Data Protection Board, breach notification, consent framework, Rs. 250 crore penalty per violation.	Gazette of India, August 11, 2023 (Annexure P-3)	Act enacted.	Board NEVER constituted. Rules NEVER notified. No breach notification ever issued. InMobi and Silverpush never investigated under DPDPA. Effective protection: zero.
2024 (April)	Operation Hawk: 60 arrests, Rs. 800 crore attached. Operation Chakra-II: 43 arrests. Every arrested person is an Indian national at operational level.	ED press releases (Annexure P-10)	Money attachment; Indian operators prosecuted.	ZERO Chinese principals arrested. ZERO data recovery. ZERO extradition requests. The architects of the system, the data, and the money

Date / Period	Event	Evidence / Source	What the State Did	What the State Failed to Do
				trail's exit point remain untouched.
2024 (Full Year)	I4C/MHA: Rs. 2,140 crore lost to digital arrest in 2024 alone. 4.6 million total NCRP complaints. 2.3% conviction rate. Every digital arrest call uses stolen Aadhaar-address data.	MHA I4C Annual Report 2024; NCRB 2023 (Annexures P-8, P-13)	Awareness campaigns; I4C helpline.	CNAP not deployed. DPB not constituted. No data-specific action. The stolen data continues to be the operational backbone of every fraud call.
2025 (Full Year)	Generation 5 operations: fully AI-automated fraud, no Indian employee. Voice-cloned officials, deepfake police video. 80M KYC records now capable of generating 8 billion+ AI-personalised fraud operations.	I4C advisory 2025; CERT-In deepfake alert 2025; Kerala Cyber Dome 2025	Individual deepfake advisories issued.	No legislative response to AI-voice fraud. No DPB to handle AI-generated privacy violations. No structural intervention in any generation of the evolving threat.
March 2026	Filing of this Petition. Five years of state inaction documented. Every administrative remedy exhausted. This Hon'ble Court is the only remaining constitutional forum.	Present petition; Annexures P-1 through P-16	This Petition filed.	—

IN THE SUPREME COURT OF INDIA

EXTRA ORDINARY WRIT JURISDICTION

WRIT PETITION (CIVIL) NO. _____ OF 2025

IN THE MATTER OF:

1. NITISH KUMAR, son of Late Dilip Kumar, aged about 32 years. Permanent Address: Anita and Sons, Village Alkjara, P.O. & P.S. Jhajha, District Jamui, Bihar – 811308. Currently Residing At: D2–8206, Eco Floors, Kharar–Mohali, Punjab – 140301. Email: nkumar906099@gmail.com | Phone: 9082843142. Occupation: Technology Consultant / AI Scholar & National Cyber Security Scholar. PAN: KNPPK5962K | Aadhaar: 7538 5441 4077 | Annual Income: Rs. 28 Lakhs p.a.

...Petitioner-in-Person

Versus

1. Union of India

Through the Secretary, Ministry of Electronics and Information Technology (MeitY), Electronics Niketan, 6 CGO Complex, Lodhi Road, New Delhi – 110 003. Email: secy-miety@gov.in | Phone: 011-24301851

2. Reserve Bank of India

Through the Governor, Central Office, Shahid Bhagat Singh Road, Mumbai – 400 001. Email: helpdeskrtirbi@rbi.org.in | Phone: 022-22610948

3. Ministry of Home Affairs / I4C

Through the Secretary (MHA), North Block, Central Secretariat, New Delhi – 110 001. Email: secy-mha@nic.in | Phone: 011-23092011

4. Telecom Regulatory Authority of India

Through the Chairman, Mahanagar Doorsanchar Bhawan, 20 Ashoka Road, New Delhi – 110 002. Email: advlf@trai.gov.in | Phone: 011-23220209

5. Data Protection Board of India (To Be Constituted)

Through the Secretary, MeitY (as competent authority until Board is constituted), New Delhi – 110 003.

6. Enforcement Directorate

Through the Director, Lok Nayak Bhawan, Khan Market, New Delhi – 110 003. (For directions on data recovery mandate and extradition proceedings.)

7. InMobi Technologies Pvt Ltd

469, 100 Feet Road, Koramangala 1A Block, Bengaluru – 560 034. | InMobi Pte Ltd, Singapore — to be served through MeitY as competent authority under IT Act.

8. Silverpush Technologies Pvt Ltd

Registered Office: [As per MCA21 records, Noida / Delhi NCR], Uttar Pradesh.

9. Google India Pvt Ltd

Bagmane Tech Park, CV Raman Nagar, Bengaluru – 560 093. (As operator of Google Play Store and host of SDK-embedded applications in the Indian market.)

10. All State Governments / Union Territories

Through respective Chief Secretaries / Directors General of Police. To be served through Ministry of Home Affairs, North Block, New Delhi – 110 001.

...All Contesting Respondents

WRIT PETITION (CIVIL) — PUBLIC INTEREST LITIGATION UNDER ARTICLE 32 | NATIONAL IMPORTANCE | MATTER OF EXTREME URGENCY | CRIMINAL ELEMENT: PRAYER FOR INVESTIGATION, FIR REGISTRATION, EXTRADITION PROCEEDINGS AND DATA RECOVERY

TO,

The Hon'ble Chief Justice of India and His Companion Justices of the Hon'ble Supreme Court of India.

HUMBLE PETITION OF THE PETITIONER ABOVE-NAMED

MOST RESPECTFULLY SHOWETH:

1. INTRODUCTION

1.1 That the present Writ Petition under Article 32 of the Constitution of India is filed in public interest. It raises questions of constitutional importance that have no precedent in their combination: the systematic theft of 80 million Indian citizens' biometric and identity data by a foreign-directed criminal enterprise; the deployment of that data over five years as a weapon for mass financial extortion and psychological torture; the complete failure of the State to recover the data, extradite its principal architects, or operationalise the statutory protection that Parliament created; and the daily, quantifiable, irreversible worsening of this situation while the State remains focused on money attachment alone.

1.2 That this Petition does not challenge a policy choice. It challenges the constitutional validity of a specific, documented pattern of State omission — and it does so with evidence, not argument alone. Every failure identified in this Petition is traceable to a specific agency, a specific statutory power that was not exercised, and a specific document showing the agency was aware of the need.

THE PETITION IN ONE PARAGRAPH — FOR THE RECORD OF THIS HON'BLE COURT

Between 2017 and 2022, Chinese-directed criminal enterprises stole the complete biometric and identity records of 80 million+ Indian citizens through three documented channels: (1) Android loan applications that harvested contacts, SMS, location, photographs, and bank data through device permissions with no legitimate lending purpose; (2) shell NBFC KYC collection fronts that harvested Aadhaar, PAN, facial biometric, and bank account data from loan applicants; and (3) adtech SDKs — specifically InMobi (subject of FTC Consent Order, 2016) and Silverpush (subject of FTC Warning Letters, 2016) — that conducted covert device surveillance. The principal Chinese architect of this operation, known as 'Jeffrey Zhu' (Zhu Wei), departed India before a Look Out Circular was issued, carrying the master database. India has filed zero extradition requests. The data remains on Chinese servers and is being actively used to perpetrate digital arrest fraud (Rs. 2,140 crore loss in 2024 alone), AI sextortion, and Telegram investment fraud against the same Indian citizens it was stolen from. Every State investigation has been directed at money. Not one has been

directed at the data. The Data Protection Board — enacted in 2023 — has never been constituted. Five years of intelligence submissions by this Petitioner to six government bodies have produced zero investigative responses. This Petition asks this Hon'ble Court to direct the State to do what it has never done: pursue the data, pursue the architects, and protect the 80 million citizens whose informational identity is in hostile hands today.

1A. PIL GUIDELINES UNDER ORDER

i. Full Name & Identification:

I, Nitish Kumar, son of Late Dilip Kumar, aged about 32 years, resident of Village Alkjara, P.O. & P.S. Jhajha, District Jamui, Bihar – 811308, presently residing at D2–8206, Eco Floors, Kharar–Mohali, Punjab – 140301, do hereby declare that my email ID is nkumar906099@gmail.com, mobile number is 9082843142. My occupation is Technology Consultant / AI Scholar & National Cyber Security Scholar. PAN: KNPPK5962K, Aadhaar: 7538 5441 4077, Annual Income approximately Rs. 28 Lakhs per annum.

ii. Nature & Extent of Personal Interest:

I have no personal interest in the subject matter of this petition. My only interest is as a citizen of India and National Cyber Security Scholar who has documented this ecosystem, submitted intelligence to multiple government authorities without response, and now approaches this Hon'ble Court as the only remaining constitutional forum for 80 million Indian citizens whose data rights are being violated daily.

iii. Facts Constituting Cause of Action:

The cause of action arises from: (a) the systematic exfiltration of 80 million+ Indian citizens' biometric data through documented technical channels; (b) the State's five-year failure to recover or destroy that data, extradite its principal architects, or enforce existing statutory protections; (c) the ongoing weaponisation of the stolen data causing Rs. 2,140 crore in losses in 2024, 83+ deaths by suicide, and daily psychological torture of Indian citizens; and (d) the non-response to

specific intelligence submitted by the Petitioner. The cause of action is continuing — it worsens every day and every hour.

iv. Nature of Injury:

The injury is present, daily, and irreversible. 80 million citizens' complete identity profiles are in criminal hands. Each stolen KYC record can generate 100 mule financial accounts and unlimited AI-personalised fraud scripts. 80 million records = 8 billion potential fraudulent operations. Every hour of delay is not abstract — it corresponds to 105 new digital arrest calls, Rs. 8.5 crore in coerced transfers, and an incrementally permanent erosion of 80 million citizens' digital security.

v. Representation to Government Authorities:

Detailed intelligence was submitted to MeitY, I4C/MHA, RBI, TRAI, PMO, and NCSC between 2022 and 2025. All submissions received standard acknowledgements or no response. Zero investigative action was triggered. Copies are at Annexures P-14 and P-15. Administrative remedy is exhausted.

vi. Other Litigation: None pending.

vii. Personal Gain / Private Motive: None. Filed purely in public interest.

viii. Similar Petition: No similar petition filed before this or any other Court.

1B. Maintainability, Locus & Cause of Action

i. Maintainability:

Maintainable under Article 32 as it seeks enforcement of Articles 14, 19(1)(a), and 21. This Hon'ble Court has in Bandhua Mukti Morcha (1984) and Puttaswamy (2017) confirmed that systematic violations of fundamental rights — including the right to informational privacy — are remediable by PIL under Article 32.

ii. Locus Standi:

The Petitioner has locus standi as a citizen, taxpayer, and professional cyber security scholar who has formally submitted evidence to government authorities and received no response. As held in S.P. Gupta v. UOI (1981), locus standi in PIL extends to any public-spirited citizen. The Petitioner additionally has standing as a whistleblower-like figure whose intelligence submissions are themselves a subject of this Petition. This Court has a duty to protect such citizens under PUCL v. UOI (1997) and Mahender Chawla v. UOI (2019).

iii. Cause of Action:

The cause of action arises from the five-year documented pattern of State omission described in the Synopsis and List of Dates. It is a continuing cause of action — it does not require a specific triggering event; it is renewed every day the data remains in hostile hands, every day the DPB is not constituted, every day Jeffrey Zhu faces no extradition request, and every day 105 Indian citizens per hour receive digital arrest calls enabled by their own stolen data.

Conclusion: This Petition is maintainable; the Petitioner has locus standi; and the cause of action is not only established but is continuing at a quantifiably increasing rate of harm.

2. FACTS CONSTITUTING THE CAUSE OF ACTION

2.1 That this Petition under Article 32 is filed in public interest against the systematic exfiltration of the personal, biometric, and financial data of 80 million+ Indian citizens; the complete failure of the State to recover, destroy, or otherwise remediate that data; the impunity of Chinese national principal accused who have absconded; the non-operationalisation of the DPDPA 2023; and the ongoing AI-amplified weaponisation of stolen data causing daily, quantifiable harm to Indian citizens. (Ref: Appendix, pages 36–75.)

2.2 That the Petitioner is a National Cyber Security Scholar who has formally submitted intelligence on this ecosystem to six government bodies between 2022 and 2025, without investigative response, and brings this evidence-backed, techno-legal petition with no personal interest other than the constitutional duty of a citizen who possesses specific, documented evidence of a national data emergency.

2.3 HOW THE DATA WAS HARVESTED — THE THREE-LAYER TECHNICAL MECHANISM:

LAYER 1 — ANDROID PERMISSIONS EXPLOITATION:

2.3.1 That Chinese-backed predatory loan applications were distributed on the Google Play Store and via direct APK links. Each application demanded device permissions wholly disproportionate to any lending function, as follows:

Permission Demanded	Any Legitimate Lending Purpose?	Actual Use Documented in Evidence	Evidence Source
READ_CONTACTS	None. No legitimate lender needs a borrower's full address book.	Entire contact database extracted (names, numbers, relationships). Used for: harassment calls to all contacts on default; sold in dark web KYC bundles.	ED prosecution forensic exhibits; CloudSEK APK analysis (Annexure P-11)

Permission Demanded	Any Legitimate Lending Purpose?	Actual Use Documented in Evidence	Evidence Source
READ_SMS	Claimed: detect OTP (one SMS).	Continuous monitoring of ALL SMS — bank balance alerts, transaction confirmations, personal communications — mapping complete financial and personal life.	Group-IB India network analysis 2022 (Annexure P-11)
ACCESS_FINE_LOCATION (GPS)	None.	Real-time + historical GPS tracking. Used to identify employer address, isolation windows for pressure calls. Sold to behavioral data brokers.	ED prosecution exhibits; Group-IB India 2022
READ_CALL_LOGS	None.	Complete call history. Used to map every personal and professional relationship for targeted coercive contact.	ED forensic analysis
CAMERA + READ_EXTERNAL_STORAGE	One-time selfie for KYC (camera only).	Bulk harvest of ALL stored photographs. Personal, family, intimate images became source material for AI deepfake sextortion from 2022.	Maharashtra Cyber 2023 annual report; Kerala Cyber Dome 2025 (Annexure P-8)
RECORD_AUDIO	None.	Microphone access enabled Silverpush-type ultrasonic beacon detection during background processing. Some variants activated during idle state.	CloudSEK 2022; Silverpush FTC Warning Letters 2016 (Annexure P-5)
GET_ACCOUNTS	Claimed: link bank for disbursement.	Revealed ALL Google, social media, email accounts on device — used for cross-platform identity mapping and account takeover.	ED prosecution exhibits
PROCESS_OUTGOING_CALLS	None.	Ability to intercept and record outgoing calls without user knowledge or consent.	Forensic APK reverse engineering; ED exhibits

2.3.2 That the combination of the above permissions constitutes comprehensive surveillance-level device access. There is no world in which a lender — legitimate or otherwise — requires simultaneous access to a borrower's complete address book, all SMS messages, GPS history, all

photographs, microphone, and all linked accounts. This permission bundle was the designed surveillance architecture. The loan product was the delivery mechanism.

LAYER 2 — SHELL NBFC KYC COLLECTION FUNNEL:

2.3.3 That borrowers who applied for loans submitted — believing they were dealing with a regulated lender — their Aadhaar number, PAN, bank account number and IFSC code, a live selfie photograph (facial biometric), and proof of address. This is the most sensitive information an Indian citizen possesses. It was submitted to shell entities — Cred Fintech Pvt Ltd, Acemoney India Ltd, Transerve Technologies, HiWe Finance, and others — which were not genuine lenders but KYC data collection fronts. The data was transmitted directly to Chinese-controlled server clusters. Even after these entities were prosecuted, no data destruction order was ever issued. The data remains.

LAYER 3 — ADTECH SDK SURVEILLANCE:

2.3.4 That the third harvesting layer operated invisibly through the InMobi SDK (FTC Consent Order 2016, Case C-4530: covert WiFi geolocation tracking of 100 million devices including children, without consent, even when GPS was OFF) and the Silverpush SDK (FTC Warning Letters 2016: ultrasonic audio beacon technology triggering device microphone access). Both SDKs were embedded in hundreds of Indian consumer applications. Both have documented foreign regulatory findings of covert user surveillance. Neither triggered any Indian investigation, enforcement action, or user notification.

2.4 THE DATA PIPELINE — FROM DEVICE TO CHINESE SERVER:

DOCUMENTED DATA PIPELINE — RECONSTRUCTED FROM ED PROSECUTION FORENSIC ANALYSIS AND GROUP-IB INDIA REPORT 2022

STEP 1 — DEVICE: App installed. Permissions accepted under coercive all-or-nothing bundle. Victim believes they are applying for a loan.

STEP 2 — COLLECTION MODULE: APK reads contacts, SMS, call logs, location, gallery, device accounts. Data compressed into encrypted JSON payload. Unique Device Fingerprint ID (DFID) assigned to victim.

STEP 3 — C2 UPLOAD: Encrypted HTTPS POST sent to hardcoded API endpoint on Alibaba Cloud (China) or AWS Singapore. Frequency: every 24–72 hours even without user interaction. Continues after loan is repaid or app is uninstalled.

STEP 4 — NBFC KYC MERGER: KYC data (Aadhaar + PAN + bank + face photo) submitted through app or NBFC form is merged with DFID record. Complete identity profile created. One record = complete digital identity of one Indian citizen.

STEP 5 — CHINESE DATABASE: Records stored in MongoDB / MySQL cluster under control of Jeffrey Zhu / Zhu Wei organisation (per ED prosecution materials). Access: principal operators + dark web broker buyers.

STEP 6 — DARK WEB SALE: 'India KYC Bundle' — Rs. 500–2,000 per 1,000 records. Verified authentic by CloudSEK through cross-matching with public records (Annexure P-11).

STEP 7 — WEAPONISATION: Records used for digital arrest calls (Aadhaar-address credibility), sextortion (photo data + AI deepfake), mule account generation (Aadhaar + PAN + bank = complete account opening kit), and Telegram investment fraud targeting (phone + behavioral profile = personalised script).

2.5 THE CHINESE ABSCONDERS — STATUS AS OF MARCH 2026:

Name / Alias	Role in Digital Dacoity	Source / Evidence	LOC Status	Interpol RCN	Extradition Request Filed?	Present Status (March 2026)	Why No Arrest: The Specific Failure
Zhu Wei / 'Jeffrey Zhu' (朱伟)	APEX: Financial controller, data pipeline architect, master database custodian, crypto exit operator. The single most important accused in this entire ecosystem.	ED PMLA prosecution complaints, Delhi ZO 2021–22; multiple state FIRs (AOR to verify ECIR nos.)	LOC issued — AFTER his departure from India. This is the primary investigative failure.	Applied to Interpol NCB. Status unconfirmed.	NONE FILED	Believed in China (Shenzhen) or Dubai. Never prosecuted. Holds master database of 80M Indian records.	LOC was issued after he departed. No extradition request under Extradition Act Section 4 (which does not require a treaty). Diplomatic silence towards China.
Liu Yang / 'Michael Yang'	Beneficial owner, PowerBank Digital Tech; oversaw operations of 3 app	ED Prosecution Complaint 2023; Karnataka Police FIR	Issued	Applied	NONE FILED	Absconded to Shenzhen. Never prosecuted.	Same structural failure: LOC issued; no follow-through on extradition. No MLAT request to

Name / Alias	Role in Digital Dacoity	Source / Evidence	LOC Status	Interpol RCN	Extradition Request Filed?	Present Status (March 2026)	Why No Arrest: The Specific Failure
	networks in India.	(loan app network)					Singapore/UAE where corporate entities registered.
Zhuang Wei / 'David Zhuang'	Financial controller; fund routing from India to UAE then China via USDT crypto.	ED/SFIO Joint Probe 2024; Delhi EOW FIR	Issued	Applied	NONE FILED	Believed in Dubai. UAE cooperation formally requested; no result.	Extradition Act Section 4 (without treaty) never invoked for UAE despite bilateral relations.
Wang Xin / 'Sunny Wang'	Apex operator for second-tier app cluster; beneficial owner of 5+ apps.	Multiple state FIRs; ED Diffusion Notice	Diffusion notice only	Diffusion only	NONE FILED	Believed in Hong Kong. Not prosecuted.	Diffusion notice is not an extradition request. No criminal proceedings initiated in any foreign jurisdiction.
Chen Wei / 'James Chen'	IT infrastructure head; managed C2 backend servers physically located in India (2018–2020).	Karnataka Police FIR 2022; ED PMLA	Issued	Applied	NONE FILED	Believed in Shenzhen. Never tried.	Departed before prosecution could commence. India-China extradition treaty absence used as excuse despite Section 4 being available.
Wang Fang (female)	Call centre setup and coordination, Pune operations.	Pune Cyber Cell FIR 2021	N/A — arrested	N/A	N/A	DEPORTED to China, March 2021, WITHOUT criminal prosecution before deportation. Chinese authorities took no recorded action.	Deportation without prosecution = impunity by process. India voluntarily surrendered its only leverage — criminal prosecution — in exchange for nothing.
6 unnamed	Operational call centre staff, Chinese loan	Telangana Police FIR 2020	N/A — arrested	N/A	N/A	DEPORTED December 2020 without	Same pattern: deport instead of prosecute. Identity records

Name / Alias	Role in Digital Dacoity	Source / Evidence	LOC Status	Interpol RCN	Extradition Request Filed?	Present Status (March 2026)	Why No Arrest: The Specific Failure
Chinese nationals	app, Hyderabad.					criminal conviction.	held by ED but no criminal proceedings before deportation.

2.6 THE EVOLVING THREAT — SAME ARCHITECTURE, NEW NAMES:

2.6.1 That the State's response architecture is fundamentally name-dependent. When an app is banned, its name is banned. Its backend server, its SDK code, its NBFC credential, and its Chinese operator continue. A new app appears within 48–72 hours. This is not inference — it is the documented pattern of five successive generations of the same operation, as follows:

Generation	Period	Method	State Response	Time to Reconstitute	What Continued Unchanged
Gen 1	2017–2020	Play Store APK with permissions bundle. ~600 apps.	Individual Play Store removals from 2020 onward.	48–72 hours (new developer account, same backend).	Backend C2 servers, data collection SDK, NBFC credential, Chinese operators.
Gen 2	2020–2022	Direct APK via WhatsApp + SMS links; sideloading. Bypasses Play Store entirely.	No effective response — WhatsApp distribution outside MeitY's app store enforcement reach.	Instant — no Play Store approval required.	Everything. Gen 2 was identical to Gen 1 in technical architecture.
Gen 3	2022–2023	Play Store app with acquired legitimate NBFC name displayed (RBI 2022 mandate compliance). Same data pipeline.	RBI enforcement against shell NBFCs (Cred Fintech, Acemoney). App removed after complaint.	48–72 hours (new NBFC credential purchased).	Backend servers, SDK, Chinese operators, data exfiltration pipeline.
Gen 4	2023–2025	Telegram-based lending. No app. KYC collected via Telegram bot. No Android permissions needed — victim voluntarily uploads Aadhaar to bot.	I4C advisories. Individual Telegram channel takedown requests. 34% compliance by Telegram.	Instant — new Telegram bot deployed in minutes.	Chinese operators, data collection, backend database merger, dark web sale.

Generation	Period	Method	State Response	Time to Reconstitute	What Continued Unchanged
Gen 5	2025–2026	Fully AI-automated. No Indian employee. Voice-cloned officials, deepfake police video, automated chatbot fraud. Operates from UAE/Cambodia/China servers.	Individual deepfake advisories. No structural intervention.	Never reconstitutes — it was never disrupted. The infrastructure is now entirely outside Indian jurisdiction.	Everything. The architecture is now permanent and unreachable without diplomatic and international legal intervention.

2.6.2 That the pattern above demonstrates with mathematical certainty that app-level enforcement is insufficient. The only interventions that would actually break this cycle are: (a) targeting the backend server infrastructure and the data it holds; (b) prosecuting or extraditing the Chinese principal operators who control the infrastructure; and (c) creating a structural regulatory mechanism — through the Data Protection Board, real-time NBFC verification, and mandatory SDK audits — that makes the initial data harvesting impossible or immediately detectable. This Petition asks for all three.

2.7 THE STATE'S COMPLETE FAILURE ON DATA — DOCUMENTED:

2.7.1 That from 2020 to March 2026, not one of the following data-specific remedial actions has been taken by any Respondent:

(a) A court order, ED attachment order, or diplomatic note demanding the return or forensic destruction of the exfiltrated Indian citizen data held on servers outside India.

(b) A formal extradition request under Sections 3 or 4 of the Extradition Act, 1962, against any named Chinese national principal accused — including Jeffrey Zhu / Zhu Wei.

(c) A forensic investigation specifically directed at the data pipeline and backend server infrastructure as distinct from the money flows.

(d) Notification to any of the 80 million+ affected Indian citizens that their biometric data was exfiltrated.

(e) Any regulatory action against InMobi or Silverpush for their FTC-documented covert surveillance of Indian users.

(f) Constitution of the Data Protection Board under the DPDPA 2023, enacted specifically to provide enforcement mechanisms for exactly this kind of data harm.

(g) Any investigative action in response to the specific intelligence submitted by the Petitioner to six government bodies between 2022 and 2025.

2.7.2 That the evidence for each of these failures is not circumstantial — it is the absence of any public record, any press release, any parliamentary response, any court order, any RTI-accessible document showing that any of the above actions were taken. The negative is provable by search, and the Petitioner invites this Hon'ble Court to direct Respondents to produce any such document if it exists.

3. QUESTIONS OF LAW

a) Article 21 — Right to Privacy Through Mass Data Theft —

Whether the systematic covert harvesting of personal, biometric, and financial data of 80 million+ Indian citizens through the three-layer architecture described in paragraph 2.3 — without consent, without legal basis, and without proportionality — constitutes an ongoing violation of Article 21 as interpreted in Puttaswamy (2017) 10 SCC 1?

b) Article 21 — Right to Life: Deaths and Torture Caused by Weaponised Data —

Whether the use of stolen biometric data to perpetrate digital arrest torture (Rs. 2,140 crore loss 2024; 83+ documented deaths), AI sextortion, and loan app harassment constitutes a violation of the right to life — and whether the State's failure to act on this, having been notified from 2021, amounts to a continuing constitutional tort for each death and each act of torture caused?

c) Article 14 — Arbitrary Investigation Architecture: Money vs. Data —

Whether the State's investigative response — which pursues money attachment (Rs. 800+ crore in Operation Hawk) while entirely ignoring the exfiltrated data — is arbitrary and violates Article 14; and whether the prosecution of Indian operational-level accused while Chinese principal architects enjoy complete impunity is discriminatory without rational basis?

d) Article 14 — Eight Years of Inaction on FTC-Documented Adtech Violations —

Whether MeitY's failure, for eight years, to take any action in response to binding FTC findings against InMobi and warning letters against Silverpush — for documented covert surveillance of Indian citizens — is arbitrary and violates Article 14?

e) Article 19(1)(a) — Mass Surveillance Chilling Effect —

Whether the documented ambient surveillance of 80 million Indian citizens' devices — their data in criminal hands, their Aadhaar data weaponised for impersonation, their photographs weaponised for sextortion — creates an unconstitutional chilling effect on digital expression, communication, and civic participation, violating Article 19(1)(a)?

f) Data Sovereignty — Extension of Ram Jethmalani Doctrine —

Whether this Hon'ble Court should recognise that stolen citizen biometric data held by foreign criminal enterprises constitutes a national asset recoverable under the same constitutional logic as illicit funds held abroad — and that the State has an affirmative constitutional obligation to pursue its return or destruction?

g) DPDPA Non-Operationalisation — Mandamus —

Whether the non-constitution of the Data Protection Board and non-notification of implementing rules under the DPDPA 2023, two years after enactment, constitutes an abdication of statutory duty remediable by Writ of Mandamus?

h) Evolving Threat — Structural Judicial Intervention —

Whether this Hon'ble Court, faced with a documented five-generation pattern of threat evolution in which name-level enforcement has demonstrably failed, may exercise its jurisdiction under Articles 32 and 142 to issue structural directions targeting the data pipeline infrastructure, the adtech SDK architecture, and the extradition of principal architects — directions that address the permanent infrastructure rather than its successive manifestations?

i) Failure to Act on Intelligence — Accountability and Remedy —

Whether the documented failure of six government bodies to take any investigative action on specific, expert intelligence submissions over three years constitutes a constitutional omission for which this Court may direct accountability and a mandatory, time-bound response?

4. GROUNDS

a) Violation of Article 21 — Three-Layer Data Theft as Continuing Privacy Violation

That the triple-layer data harvesting architecture documented in paragraph 2.3 — (Layer 1) Android permission exploitation harvesting contacts, SMS, location, photographs, and microphone data without legitimate lending purpose; (Layer 2) shell NBFC KYC funnels collecting Aadhaar, PAN, facial biometric, and bank data under false pretence; and (Layer 3) adtech SDK covert surveillance (InMobi: WiFi geolocation without consent, FTC Consent Order 2016; Silverpush: audio beacon microphone access, FTC Warning Letters 2016) — constitutes an ongoing, State-enabled violation of the fundamental right to informational privacy established in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1. The constitutional triple test of legality, legitimate aim, and proportionality is not satisfied by any element of this data collection — there is no legal basis, no lending purpose, and no proportionality in harvesting an entire address book and photograph gallery for a short-term loan. The State had statutory power to prevent this under IT Act Section 43A and the RBI Act. It did not act. Every day of inaction is a renewed constitutional violation.

b) Violation of Article 21 — Right to Life: Weaponised Data Causing Deaths

That the weaponisation of stolen biometric data to perpetrate (a) digital arrest fraud — Rs. 2,140 crore extracted in 2024 alone, with victims held in psychological captivity for up to 26 days using their own Aadhaar-address details for false credibility; (b) loan app harassment — 83+ documented deaths by suicide between 2020 and 2023, using harvested contact lists and photographs for coercive calls to family and employers; and (c) AI sextortion — using harvested photographs processed through deepfake generators — constitutes a violation of Article 21 in its most direct sense. In Paschim Banga Khet Mazdoor Samity v. State of WB (1996), this Court held that denial of protection violates Article 21. The State was specifically notified of the data theft from 2021 and took no data-specific action. Every death and every psychological torture that occurred after 2021 is a harm for which the State bears constitutional liability through its documented omission.

c) Violation of Article 14 — Data Ignored, Money Pursued: Arbitrary Investigation

That the State's investigative response violates Article 14 in its treatment of two categories of harm arising from the same criminal enterprise as if they were not equivalent: (a) financial harm — aggressively pursued under PMLA, Rs. 800+ crore attached in Operation Hawk, 103 total arrests; and (b) data harm — 80 million biometric records exfiltrated and actively weaponised, never investigated as a distinct remedial objective, zero data recovery actions, zero data destruction orders. The data causes greater, more permanent, and more exponentially scaling harm than the money — in the AI era, each record can generate 100 mule accounts. There is no rational basis for this discrimination. It is arbitrary in the sense of E.P. Royappa v. State of TN (1974).

d) Violation of Article 14 — Prosecution of Workers, Impunity of Architects

That the prosecution record of 2019–2026 reveals a stark and irrational pattern: every person convicted or charge-sheeted is an Indian national at the call centre, mule account, or mid-level criminal enterprise level. Every Chinese national who designed the data harvesting system, controlled the backend, exfiltrated the data, and monetised it — including Zhu Wei ('Jeffrey Zhu'), Liu Yang, Zhuang Wei, Wang Xin, and Chen Wei — has either absconded without extradition proceedings or been deported without criminal trial. This is arbitrary discrimination without rational basis — the persons who designed and profited most from the crime face zero legal consequence, while those who answered phones face prosecution. It creates a perverse incentive that guarantees the next generation of the operation will be structured identically.

e) Violation of Article 19(1)(a) — Ambient Surveillance as Chilling Effect

That when 80 million Indian citizens know their contact lists have been exfiltrated, their SMS history is in criminal hands, their photographs are available to every AI sextortion operator on the dark web for Rs. 99–499 per image, and their own Aadhaar number will be cited by the next digital arrest caller as 'proof' of investigation — they cannot freely communicate, freely transact, or participate in digital civic life without ambient fear. This is the constitutional chilling effect recognised in Shreya Singhal v. Union of India (2015). The State's failure to remediate this surveillance creates a condition in which Article 19(1)(a) rights are exercised, if at all, under continuous coercion.

f) Data Sovereignty — The Ram Jethmalani Extension

That in Ram Jethmalani v. Union of India (2011) 8 SCC 1, this Court recognised that illicit assets of Indian citizens held abroad impose an affirmative constitutional obligation on the State to pursue recovery through all available legal mechanisms. Personal biometric data generated by Indian citizens — Aadhaar numbers, facial biometrics, PAN numbers, bank account data — is a national asset in the most fundamental constitutional sense. It was stolen through criminal means by foreign-directed enterprises and placed on foreign servers. It is being used to harm its original owners every day. The State has an affirmative, positive constitutional obligation — stronger than the obligation for money, because data harm is more permanent than financial harm — to pursue, through diplomatic notes, MLAT requests, Extradition Act Section 4 proceedings, and UNCAC cooperation, the return or verified forensic destruction of this data. This obligation has never been discharged.

g) <u>Failure to Operationalise DPDPA 2023 — Abdication of Statutory Duty</u>

That the Digital Personal Data Protection Act, 2023, enacted on August 11, 2023, creates the Data Protection Board with enforcement powers, mandates breach notification within 72 hours, establishes a consent framework, and provides penalties of up to Rs. 250 crore per violation. These provisions exist specifically to address the harm described in this Petition. The non-constitution of the Board, non-notification of implementing rules, and non-operationalisation of the breach notification mechanism — more than two years after enactment — constitutes a specific, enforceable, documented abdication of statutory duty. A Writ of Mandamus is the only appropriate remedy. The 80 million citizens whose data was stolen are also the citizens to whom the Act's protections were promised.

h) <u>Structural Failure: App-Level Enforcement Cannot Stop Infrastructure-Level Crime</u>

That the five-generation pattern of threat evolution documented in paragraph 2.6 demonstrates that the State's current enforcement architecture — removing individual apps, arresting individual call centre workers, attaching individual money transfers — is structurally incapable of addressing a threat that reconstitutes itself within 48–72 hours under a new name. This Court has jurisdiction under Articles 32 and 142 not only to remedy past harm but to prevent continuing and future harm. It has exercised this jurisdiction through structural directions in environmental cases (T.N. Godavarman; M.C. Mehta — Ganga Pollution), in institutional reform cases (Vineet Narain), and in fundamental rights protection cases (Vishaka). This Petition asks for the same structural intervention: directions that address the permanent infrastructure of the threat — the

data pipeline, the backend servers, the adtech SDKs, and the Chinese principals — not merely its successive app-level manifestations.

i) State's Positive Constitutional Duty: Omission as Constitutional Tort

That this Court has established in M.C. Mehta v. Union of India (Oleum Gas Leak, 1987), Nilabati Behera v. State of Orissa (1993), and NALSA v. Union of India (2014) that the State bears a positive constitutional obligation to protect citizens from violations of fundamental rights by non-State actors where: (a) the violation is systematic and large-scale; (b) the State has the regulatory capacity to prevent it; and (c) the State omits to exercise that capacity. All three conditions are met here with specificity and documented evidence. The State had power under IT Act Section 43A to mandate minimum-necessary permissions. It had power under the RBI Act to require real-time NBFC verification. It had power under PMLA to seek data destruction as a condition of settlement. It had power under Extradition Act Section 4 to extradite without a treaty. In each case it omitted to act. Each omission, documented in this Petition, is a constitutional tort.

5. MAIN PRAYER

Under Article 32 read with Article 142 of the Constitution of India, the Petitioner most humbly prays that this Hon'ble Court may be pleased to:

(a) <u>DATA RECOVERY AND DESTRUCTION MANDATE — THE PRIMARY RELIEF (Novel Constitutional Direction)</u>

Issue a Writ of Mandamus commanding Respondents Nos. 1, 3, and 6 (MeitY / MHA / ED) to: (i) Within 30 days, file a comprehensive inventory of all known databases, server clusters, and data repositories outside Indian territory containing exfiltrated Indian citizen data; (ii) Within 60 days, issue formal diplomatic Note Verbale to the Governments of China, UAE, and Cambodia specifically naming Jeffrey Zhu / Zhu Wei, Liu Yang, Zhuang Wei, Wang Xin, and Chen Wei — demanding return or forensically verified destruction of all Indian citizen personal data under their control; (iii) Within 90 days, file MLAT requests for all countries with applicable agreements seeking freezing and forensic destruction of data on servers in those jurisdictions; (iv) File quarterly compliance reports before this Court.

Legal basis: Art. 21 (Puttaswamy 2017); Art. 32; Ram Jethmalani v. UOI (2011) 8 SCC 1 — affirmative State duty to recover national assets held abroad, extended to stolen citizen data; Art. 142 — complete justice.

(b) <u>EXTRADITION AND LOC ACCOUNTABILITY</u>

Issue a Writ of Mandamus commanding Respondents Nos. 1 and 3 to: (i) Within 30 days, file a complete status report on all LOCs, RCNs, and extradition proceedings for every Chinese national accused; (ii) Within 60 days, initiate formal extradition proceedings under Section 4 of the Extradition Act, 1962 — which does not require a treaty — against Zhu Wei ('Jeffrey Zhu'), Liu Yang, Zhuang Wei, Wang Xin, and Chen Wei; (iii) Issue a formal diplomatic communication to Beijing specifically naming each accused.

Legal basis: Extradition Act 1962, Sections 3 & 4; Art. 21 (continuing harm from absconding accused); Art. 14 (discriminatory impunity); Vineet Narain v. UOI (1998) — Court-monitored investigation.

(c) <u>COURT-DIRECTED SIT INVESTIGATION INTO DATA PIPELINE</u>

Issue a direction for constitution of a Multi-Agency SIT specifically mandated to investigate: (i) The complete technical architecture of the data harvesting pipeline including SDK data collection and C2 server infrastructure; (ii) The quantum and present location of exfiltrated Indian citizen data; (iii) Criminal liability of InMobi, Silverpush, and app store operators for their role in the surveillance infrastructure; (iv) The circumstances and any intelligence failure surrounding Jeffrey Zhu's departure before LOC issuance. SIT to file initial report within 12 weeks, thereafter every 6 weeks.

Legal basis: Art. 32, 142; Vineet Narain (1998) — Court-monitored probe; M.C. Mehta Oleum (1987) — enterprise liability; BNS 2023 Sections 316–318.

(d) ARREST-BY-ARREST DATA ACCOUNTABILITY AFFIDAVIT

Direct Respondents 3 and 6 (MHA/I4C and ED) to file, within 45 days, an affidavit documenting for EVERY arrest and seizure in Chinese loan app cases (2019–2026): (i) Number of mobile devices seized; (ii) App permissions active on each seized device; (iii) Whether harvested data was forensically traced; (iv) Whether any data recovery or destruction order was made — and if not, the specific reasons; (v) Status of every Chinese national named in PMLA prosecution complaints as of March 2026.

Legal basis: Art. 14 — arbitrary data-blindness of investigation; Art. 32 — Court's accountability jurisdiction; PMLA Section 8 — attachment of all proceeds including data.

(e) INMOBI AND SILVERPUSH BACKGROUND VERIFICATION AND ENFORCEMENT

Direct Respondent No. 1 (MeitY) to: (i) Within 30 days, formally investigate whether InMobi and Silverpush violated IT Act Section 43A and IT Rules 2011 through FTC-documented covert surveillance; (ii) Within 45 days, require both entities to file affidavits disclosing: (a) all data collected from Indian devices since 2014; (b) present location and custodian of all such data; (c) data sharing agreements with foreign entities; (d) full list of Indian applications in which SDKs were embedded; (iii) Issue notification to affected Indian users; (iv) Initiate penalty proceedings under IT Act Section 43A.

Legal basis: IT Act 2000, Section 43A; IT Rules 2011; DPDPA 2023, Section 8; FTC Consent Order C-4530 (constructive notice); Art. 14 — 8 years of inaction on documented violation.

(f) FULL GOVERNMENT ACCOUNTABILITY REPORT — 2014 TO MARCH 2026

Direct all Respondents to jointly file a comprehensive chronological report within 45 days documenting: (i) Every action taken from 2014 to March 2026 specifically directed at data protection in the context of loan app and SDK surveillance; (ii) Specific action taken on the Petitioner's intelligence submissions (Annexures P-14, P-15) — name the officer, date of receipt, action taken, reason if no action; (iii) Every instance where extradition was considered, requested, or declined; (iv) Why, despite 80 million KYC records documented in dark web circulation from 2021, no data recovery or victim notification action was ever initiated.

Legal basis: Art. 32 (enforcement jurisdiction); Art. 142 (complete justice); S.P. Gupta v. UOI (1981) — right to know; continuing mandamus.

(g) DPDPA OPERATIONALISATION UNDER COURT SUPERVISION

Issue a Writ of Mandamus directing: (i) Data Protection Board constituted within 60 days; (ii) All implementing rules under DPDPA 2023 notified within 90 days; (iii) Breach notification issued to 80M affected citizens within 120 days; (iv) Compliance affidavits at 30/60/90 day intervals before this Court.

Legal basis: DPDPA 2023, Sections 6, 8, 18, 33; Art. 21 (Puttaswamy — right to informational privacy requires enforcement mechanism); Vishaka v. State of Rajasthan (1997).

(h) REAL-TIME NBFC VERIFICATION API

Direct RBI to create a publicly accessible real-time NBFC verification API within 60 days and mandate its integration into Indian app stores and payment gateways within 120 days — closing the NBFC impersonation pipeline permanently.

Legal basis: RBI Act, Chapter III-B; Art. 14 — information asymmetry enabling NBFC fraud is arbitrary; Art. 21 — citizens' right to information necessary to protect financial privacy.

(i) STRUCTURAL INJUNCTION AGAINST PATTERN RECONSTITUTION

Issue interim structural directions preventing reconstitution of the data harvesting architecture: (a) No new lending application on Indian app stores without real-time verified RBI NBFC credential; (b) Mandatory minimum-necessary permissions standard for all financial applications — any permission beyond credit assessment purpose to be specifically justified to MeitY; (c) Mandatory SDK disclosure register — every third-party SDK in a financial app must be registered with and audited by MeitY.

Legal basis: Art. 21, Art. 32, Art. 142; IT Act Section 69A (blocking orders); M.C. Mehta — precautionary principle; T.N. Godavarman — structural court directions to prevent ongoing harm.

(j) TRAI — CNAP DEPLOYMENT AND SIM FRAUD

Direct TRAI to: (i) Deploy CNAP nationally within 120 days; (ii) Mandate AI-based fraud call detection for all telecom providers within 180 days; (iii) File time-bound compliance roadmap within 3 weeks.

Legal basis: Indian Telecommunications Act 2023; Art. 21 — right to communication free from coercive impersonation.

(k) COURT-MONITORED EXPERT TECHNICAL COMMITTEE

Constitute a Court-monitored Expert Technical and Legal Committee to: forensically map the complete data exfiltration chain; estimate total volume of Indian citizen data in foreign criminal possession; assess AI-era multiplication of harm; recommend interim technical measures; audit NBFC and adtech hiring background verification failures; and report within 12 weeks, every 8 weeks thereafter.

Legal basis: Arts. 32, 142; T.N. Godavarman series; Vineet Narain (continuing mandamus).

(l) VICTIM COMPENSATION FUND

Direct the Union of India to establish within 180 days a Cyber Victim Compensation Fund with minimum statutory compensation for: families of loan app harassment suicide victims; digital arrest fraud victims; AI sextortion victims — amounts determined by the Court-appointed Committee.

Legal basis: Art. 21; Rudul Sah v. State of Bihar (1983); M.C. Mehta Oleum (1987); Nilabati Behera (1993).

(m) PROTECTION OF PETITIONER

Direct immediate protective security for the Petitioner and his family; whistleblower-like safeguards against retaliation; direction to local police to register and investigate any threats to the Petitioner.

Legal basis: Art. 21 (Maneka Gandhi 1978); PUCL v. UOI (1997); Mahender Chawla v. UOI (2019); Bandhua Mukti Morcha (1984); Whistle Blowers Protection Act 2014.

(n) RECOGNITION OF CONSTITUTIONAL TORT — DIGITAL DACOITY

Declare that the State's sustained failure from 2019 to date to prevent mass biometric data theft, recover or destroy the exfiltrated data, extradite its architects, or operationalise statutory protection — constitutes a continuing constitutional tort, herein recognised as 'Digital Dacoity' against the people of India, warranting judicial supervision until fully remedied.

Legal basis: Arts. 14, 21, 32; Nilabati Behera (1993); Puttaswamy (2017); Ram Jethmalani (2011); M.C. Mehta Oleum (1987).

(o) RESIDUAL / COMPLETE-JUSTICE CLAUSE

Pass such other orders as may be necessary for complete justice, protection of 80 million+ Indian citizens' fundamental rights, and restoration of India's data sovereignty.

Legal basis: Article 142; Article 141.

6. PRAYER FOR INTERIM RELIEFS

Pending final disposal, and in view of the documented continuing and irreversible harm described in this Petition, the Petitioner prays that this Hon'ble Court may be pleased to direct:

1. MHA/I4C to file a 30-day status report answering specifically: (a) current legal status of Jeffrey Zhu / Zhu Wei, Liu Yang, Zhuang Wei, Wang Xin, and Chen Wei; (b) whether any extradition request has been filed or is proposed; (c) what investigative action, if any, was taken on the Petitioner's intelligence submissions. Basis: Art. 32; Vineet Narain (1998); the most fundamental accountability obligation — the State must account for what it has done about the named architects of this crime.

2. InMobi Technologies Pvt Ltd and Silverpush Technologies Pvt Ltd to file affidavits within 30 days disclosing: (a) all data collected from Indian devices since 2014; (b) present location and custodian; (c) any data sharing with foreign entities. Basis: Art. 21; IT Act Section 43A; FTC Consent Order C-4530.

3. Immediate freeze on new lending application listings on Indian app stores without real-time verified RBI NBFC registration — preventing Generation 3/4/5 reconstitution while this matter is pending. Basis: Arts. 21, 32; precautionary principle; documented 48-72 hour reconstitution cycle.

4. All Respondents to file a written response to the specific intelligence submissions made by the Petitioner (Annexures P-14, P-15) within 30 days — identifying what action was taken on each submission, by which officer, on which date, and if no action was taken, the specific reasons. Basis: Art. 32; right to effective remedy; documented national security intelligence cannot be ignored without constitutional consequence.

5. TRAI to file a time-bound CNAP deployment roadmap within 3 weeks. Basis: Art. 21; 3 years have elapsed since announcement; 105 digital arrest calls per hour continue because CNAP is absent.

6. Immediate protective security for the Petitioner and his family; 48-hour threat assessment report. Basis: Art. 21; Mahender Chawla (2019); PUCL (1997).

7. VERIFICATION

I, Nitish Kumar, the Petitioner herein, do hereby verify that the contents of the above Writ Petition — including the Synopsis, List of Dates, Facts of the Case, Grounds, Questions of Law, Main Prayers, and Interim Reliefs — are true and correct to my knowledge and belief. No part of it is false, and nothing material has been concealed therefrom. The documents annexed hereto as Annexures P-1 through P-16 are true copies of their respective originals or publicly available documents. Every factual assertion relating to named individuals is based on publicly available court records, official government documents, regulatory orders, or threat intelligence reports in the public domain, as cited — and my AOR is directed to verify specific ED PMLA complaint numbers before filing.

DRAWN ON: _____ FILED BY:

Nitish Kumar

Petitioner-in-Person

Village Alkjara, P.O. & P.S. Jhajha, District Jamui, Bihar – 811308

Presently: D2–8206, Eco Floors, Kharar–Mohali, Punjab – 140301

Email: nkumar906099@gmail.com | Phone: +91-9082843142

Date: _____

AFFIDAVIT IN SUPPORT OF WRIT PETITION

I, Nitish Kumar, son of Late Dilip Kumar, aged about 32 years, resident of Village Alkjara, P.O. & P.S. Jhajha, District Jamui, Bihar – 811308, presently residing at D2–8206, Eco Floors, Kharar–Mohali, Punjab – 140301, do hereby solemnly affirm and state on oath as follows:

1. I am the Petitioner herein and am fully conversant with the facts of the case. I am competent to swear this Affidavit.

2. The statements made in the Writ Petition are true and correct to the best of my knowledge and belief. The documents annexed are true copies of their respective originals or publicly available records.

3. I have made detailed representations to MeitY, I4C/MHA, RBI, TRAI, PMO, and NCSC between 2022 and 2025, as detailed at paragraph 2.13 of the Petition and annexed as Annexures P-14 and P-15. Not one triggered investigative action. Administrative remedy is exhausted.

4. This Petition is filed bona fide, in public interest, with no personal gain or oblique motive, solely for the enforcement of the fundamental rights of 80 million+ Indian citizens whose biometric and identity data has been stolen and is being weaponised against them daily.

5. Every factual assertion in this Petition relating to named individuals and corporate entities is based on publicly available records as cited. I acknowledge that specific ED PMLA complaint reference numbers should be verified by my AOR from ED records before filing.

DEPONENT

VERIFICATION: Verified at _____ on this _____ day of _____, 202__, that the contents of the above Affidavit are true and correct to the best of my knowledge, information, and belief.

APPENDIX

CONSTITUTIONAL AND STATUTORY PROVISIONS, CASE LAW, AND ANNEXURES

Provision / Case	Bare Text / Principle	Application in This Petition
Article 14, Constitution of India	'The State shall not deny to any person equality before the law or the equal protection of the laws.'	Basis for attacking arbitrary investigation (money pursued, data ignored); discriminatory non-prosecution of Chinese principals; 8 years of inaction on FTC findings. E.P. Royappa (1974): arbitrariness = inequality.
Article 19(1)(a)	'All citizens shall have the right to freedom of speech and expression.'	Mass device surveillance creates constitutional chilling effect on digital communication. Shreya Singhal (2015); PUCL (1997).
Article 21	'No person shall be deprived of his life or personal liberty except according to procedure established by law.'	Primary article: right to informational privacy (Puttaswamy 2017); right to life against torture and death caused by weaponised data; right to digital dignity.
Article 32	'The right to move the Supreme Court by appropriate proceedings for the enforcement of the rights conferred by this Part is guaranteed.'	Jurisdiction for this Petition. 'Heart and soul of the Constitution' (Dr. Ambedkar). Bandhua Mukti Morcha (1984) — PIL jurisdiction.
Article 142	'The Supreme Court may pass such decree or order as is necessary for doing complete justice.'	Structural directions against pattern reconstitution; data recovery mandate; expert committee constitution; directions transcending ordinary mandamus.
IT Act 2000, Section 43A	Compensation for failure to protect sensitive personal data per reasonable security practices.	Basis for InMobi/Silverpush liability; MeitY's enforcement duty; data destruction as remedy.
DPDPA 2023, Sections 6, 8, 18, 33	Consent framework; breach notification; Data Protection Board; penalties up to Rs. 250 crore.	Mandamus for DPB constitution; breach notification to 80M victims; InMobi/Silverpush penalty proceedings.
PMLA 2002, Sections 5, 8, 17	Attachment, confiscation, search — extended to data as proceed/instrument of crime.	Basis for data destruction as PMLA remedy alongside money attachment.
Extradition Act 1962, Sections 3, 4	Extradition with and without formal treaty (reciprocal basis).	No treaty with China required for Section 4 extradition request. State has never invoked this.
Puttaswamy (2017) 10 SCC 1	Privacy is fundamental right; informational self-determination; triple test.	PRIMARY AUTHORITY for all data-related grounds.
Ram Jethmalani v. UOI (2011) 8 SCC 1	Affirmative State duty to recover national assets held abroad.	NOVEL EXTENSION: stolen citizen data as national asset; diplomatic demand for data return/destruction.

Provision / Case	Bare Text / Principle	Application in This Petition
M.C. Mehta v. UOI (Oleum Gas, 1987) 1 SCC 395	Absolute liability; State's positive duty against private harm; precautionary principle.	Enterprise liability for Chinese operators; State's positive duty to prevent reconstitution.
Nilabati Behera v. State of Orissa (1993) 2 SCC 746	Constitutional tort; sovereign immunity ends at gross negligence; State liability for omission.	Five-year documented omission = constitutional tort. 83+ deaths = State liability.
Vineet Narain v. UOI (1998) 1 SCC 226	Court-monitored investigation; continuing mandamus; institutional accountability.	Basis for SIT direction; accountability report; quarterly compliance before Court.
Vishaka v. State of Rajasthan (1997) 6 SCC 241	Court's power to issue binding guidelines in regulatory vacuum.	Basis for structural directions on SDK regulation, app store standards, NBFC verification API.
Mahender Chawla v. UOI (2019) 14 SCC 615	Witness Protection Scheme as enforceable law; protective measures for persons assisting justice.	Protection for Petitioner as intelligence-submitting whistleblower-like citizen.

ANNEXURES LIST

Annexure	Description	How to Obtain
P-1	Constitution of India — Articles 14, 19(1)(a), 21, 32, 142	indiacode.nic.in; Ministry of Law & Justice.
P-2	IT Act 2000 (Ss. 43A, 66, 69, 69A, 72, 72A) + IT Rules 2011	indiacode.nic.in; meity.gov.in.
P-3	Digital Personal Data Protection Act, 2023	Gazette of India, August 11, 2023; meity.gov.in.
P-4	FTC Consent Order — InMobi Pte Ltd, June 2016 (Case C-4530)	ftc.gov/legal-library/browse/cases-proceedings/152-3116-inmobi
P-5	FTC Staff Warning Letters re Silverpush SDK, March 2016	ftc.gov (search 'Silverpush warning letters 2016')
P-6	RBI Warning Circular on Unauthorized Digital Lending Apps, 2021	rbi.org.in (RBI/2020-21/116)
P-7	RBI Digital Lending Guidelines, August 2022	rbi.org.in (RBI/2022-23/111)
P-8	MHA I4C Annual Cyber Crime Data Reports 2022, 2023, 2024	cybercrime.gov.in; MHA press releases; Parliamentary Q&A records.
P-9	Parliamentary Standing Committee on Home Affairs — 237th Report	loksabha.nic.in — Committee Reports.
P-10	ED Press Releases: Operation Hawk (April 2024), Operation Chakra-II (2023)	enforcementdirectorate.gov.in

Annexure	Description	How to Obtain
P-11	CloudSEK / Group-IB India Threat Intelligence Reports re 80M KYC Data	cloudsek.com/blog; Group-IB public reports.
P-12	MEA Parliamentary Reply on Indian Nationals Repatriated from Myanmar	Lok Sabha / Rajya Sabha Starred Questions; mea.gov.in.
P-13	NCRB Crime in India 2022, 2023 — Cyber Crime Chapter	ncrb.gov.in (annual reports).
P-14	Petitioner's Representations to MeitY, RBI, MHA, TRAI, PMO, NCSC (with acknowledgements/delivery proof)	Petitioner's personal records. Include all delivery receipts.
P-15	Petitioner's Intelligence Submissions / Cyber Security Research Documents	Petitioner's personal records / research documents.
P-16	PMLA 2002 (Sections 5, 8, 17) + Extradition Act 1962 (Sections 3, 4)	indiacode.nic.in; Ministry of Law & Justice.

— END OF WRIT PETITION —

Petitioner-in-Person: Nitish Kumar | National Cyber Security Scholar | nkumar906099@gmail.com