A1

ANNEXURE 'Y'

PROFORMA FOR FIRST LISTING

SECTION _____

The case pertains to (Please tick/check the correct box):

☑ **Central Act : (Title)** Information Technology Act, 2000

Section : Sections 43A, 66, 69, 69A, 72, 72A

☑ **Central Act : (Title)** Digital Personal Data Protection Act, 2023

Section : Sections 6, 8, 18, 33 (Data Protection Board; Consent; Breach Notification; Penalty)

☑ **Central Act : (Title)** Prevention of Money Laundering Act, 2002

Section : Sections 5, 8, 17 (Attachment; Confiscation; Data as Proceeds of Crime)

☑ **Central Act : (Title)** Section 3(4) of the Extradition Act, 1962 as inserted by Act 66 of 1993

Section : Sections 3(4) (Extradition without treaty; reciprocal basis)

☑ **Central Act : (Title)** Bharatiya Nyaya Sanhita, 2023

Section : Sections 316, 317, 318 (Cheating, fraudulent deception causing property loss; computer-related offences)

☐ **Central Rule : (Title)** —

Rule No(s) : —

☐ State **Act : (Title)** —

Section : —

☐ **State Rule : (Title)** —

Rule No(s) : —

☐ Impugned **Interim Order : (Date)** —

☐ Impugned **Final Order/Decree : (Date)** —

☐ High **Court : (Name)** —

☐ Names **of Judges:** —

☐ Tribunal/**Authority : (Name)** —

1. Nature of matter : ☐ Civil ☑ Criminal *(PIL — EXTREMELY URGENT)*

2. (a) Petitioner/appellant No.1 : Nitish Kumar, AI Scholar and National Cyber Security Scholar

(b) e-mail ID: nkumar906099@gmail.com

(c) Mobile phone number: +91-9082843142

3. (a) Respondent No. 1: Union of India, through the Secretary, Ministry of Electronics and Information Technology (MeitY)

(b) e-mail ID: secy-miety@gov.in

(c) Mobile phone number: 011-24301851

4. (a) Main category classification: 48

(b) Sub classification: 48(p) — Violation of Fundamental Rights (Data Privacy / Digital Rights)

5. Not to be listed before: None specified.

6. (a) Similar disposed of matter with citation, if any, & case details: No similar matter as disposed of

(b) Similar pending matter with case details: SMW (Crl.) No. 3 of 2025 (distinct constitutional questions on different facts — not tagged).

7. Criminal Matters:

(a) Whether accused/convict has surrendered: ☐ Yes ☐ No N/A — prayers seek investigation, data recovery mandate, and extradition proceedings; no trial at this stage.

(b) FIR No.: Not registered — prayer is for Court-directed registration of FIRs under BNS 2023. **Date:** N/A

(c) Police Station: N/A

(d) Sentence Awarded: N/A — No conviction; PIL seeks investigation and systemic data protection.

(e) Sentence Undergone: N/A

(f) Whether any earlier case between the same parties is filed:

(g) Particulars of the FIR and Case: -N/A

(h) Whether any bail application was preferred earlier and decision

Thereupon: N/A

8. Land Acquisition Matters:

(a) Date of Section 4 notification: N/A — Not a land acquisition matter.

(b) Date of Section 6 notification: N/A

(c) Date of Section 17 notification: N/A

9. Tax Matters: State the tax effect: N/A — Not a tax matter.

10. Special Category (first petitioner/appellant only):

☐ Senior citizen > 65 years ☐ SC/ST ☐ Woman/child ☐ Disabled ☐ Legal Aid case In custody *(None of the above categories apply.)*

11. Vehicle Number (in case of Motor Accident Claim matters): N/A — Not a motor accident claim.

12. Decided cases with citation: **PRIMARY AUTHORITY** **1. Justice K.S. Puttaswamy (Retd.) v. Union of India** (2017) 10 SCC 1 (Nine-Judge Constitutional Bench) — *Right to Privacy is a fundamental right under Article 21. Informational privacy and data autonomy — the right to control information about oneself — is a core component. The triple test of legality, legitimate aim, and proportionality governs any interference with privacy. PRIMARY AUTHORITY for all data-related grounds in this Petition.*

CONSTITUTIONAL FOUNDATIONS **2. Kesavananda Bharati v. State of Kerala** (1973) AIR 1973 SC 1461 — *Basic Structure doctrine — fundamental rights form the unamendable core of the Constitution. Petitioner invokes this to establish that systematic State omission eroding the right to informational privacy violates the basic structure.*

Note: *No directly decided case on identical facts exists. There is no prior litigation on the same point of law. The questions of (i) stolen citizen data as a national asset attracting an affirmative recovery obligation; (ii) Article 21 liability for AI-amplified re-weaponisation of exfiltrated biometric data; and (iii) the non-invocation of Section 3(4) of the Extradition Act read with UNCAC Article 44 against named foreign cyber-crime architects — are raised for the first time before this Court.*

Nitish Kumar

A3

IN THE HON'BLE SUPREME COURT OF INDIA

WRIT PETITION (CRIMINAL) NO. _____/2026

PUBLIC INTEREST LITIGATION

UNDER ARTICLE 32 OF THE CONSTITUTION OF INDIA
IN THE MATTER OF

NITISH KUMAR …. PETITIONER

VERSUS

UNION OF INDIA & ORS …. RESPONDENT

IA NO. _____ OF 2026

APPLICATION FOR EARLY / URGENT LISTING

IA NO. _____ OF 2026

APPLICATION FOR PERMISSION TO APPEAR AND ARGUE IN PERSON

PAPER BOOK

{FOR INDEX, KINDLY SEE INSIDE}

PETITIONER IN PERSON: NITISH KUMAR

A4
Index of Record of proceedings

A5

Writ proforma- Sec on 1B

A6
Defect List

Ns1

Note Sheet

Sl No.	Particulars of documents	Page no. Of the part to which it belongs		Remarks
		Part 1 (contents of paper book)	Part II (contents of file alone)	
(i)	(ii)	(iii)	(iv)	(v)
1	Court fees			**Exempted**
2	Listing proforma	A1-A2	A1-A2	
3	Cover page of paper book		A3	
4	Index of Record of Proceedings		A4	
5	Writ proforma – Section 1B		A5	
6	Defect list		A6	
7	Note sheet		Ns1 to	
8	Synopsis and list of dates	B-H		
9	Writ petition with affidavit	1-39		
10	Appendix copy of article 136 of constitution of India	40 -47		
11	Annexure P 1 Constitution of India — Articles 14, 19(1)(a), 21, 32, and 142	48-52		
12	Annexure P 2 Information Technology Act, 2000 — Sections 43A, 66, 69, 69A, 72, 72A along with Information Technology	53-56		
13	Annexure P 3 Digital Personal Data Protection Act, 2023 (Complete Text)	57-59		
14	Annexure P4 FTC Consent Order — *In the Matter of InMobi Pte Ltd*, June 2016	60-63		
15	Annexure P5 FTC Staff Warning Letters to Developers Using Silverpush	64-67		

	SDK — March 2016			
16	Annexure P6 RBI Warning Circular — Unauthorised Digital Lending Apps (RBI/2020-21/116)	68-70		
17	Annexure P7 RBI Digital Lending Guidelines, August 2022 (RBI/2022-23/111)	71-73		
18	Annexure P8 MHA I4C Annual Cyber Crime Data Reports 2022, 2023, 2024	74-77		
19	Annexure P9 Parliamentary Standing Committee on Home Affairs — 237th Report	78-80		
20	Annexure P10 Enforcement Directorate Press Releases: Operation Hawk (April 2024) and Operation Chakra-II (CBI, August–September 2023)	81-84		
21	Annexure P11 Threat Intelligence Reports — Circulation of 80 Million+ Indian KYC Records on Dark Web	85-88		
22	Annexure P12 MEA Parliamentary Reply — Indian Nationals Repatriated from Myanmar and Southeast Asia Cyber Crime Compounds	89-91		
23	Annexure P13 NCRB “Crime in India” Reports 2022 and 2023 — Chapter on Cyber Crime Application for permission to appear and argue in person	92-94		
24	Annexure P14 Petitioner’s Representations to	95-100		

	Government Authorities — MeitY, RBI, MHA/I4C, Supreme Court of India, PMO, and NCSC (2022–2025) along with Proof of Delivery			
25	Annexure P15 Petitioner's Cyber Security Intelligence Submissions and Research Documents	101-106		
26	Annexure P16 Prevention of Money Laundering Act, 2002 — Sections 5, 8, 17; along with Extradition Act, 1962 (as amended by Act 66 of 1993) — Section 3(4)	107-111		
27	Annexure P17 Credential and certificate for Subject matter expert	112-113		
28	Application for permission to appear and argue in person		114-116	
29	Application for early / urgent listing		117-120	
30	Letter to Registrar		121-129	
31	Filing index		130-131	
32	Memo of appearance		132	
33	Declaration		133	
34	ID		134	

SYNOPSIS

1. The Petitioner is a National Cyber Security Scholar under the NSD program at Rashtriya Raksha University. Through independent analysis and detailed observation, the Petitioner has studied cyber fraud in digital lending, data exfiltration, and AI-based financial extortion, submitting evidence-backed reports to authorities. This Petition relies on ongoing monitoring and verifies documentation, not speculation. After exhausting administrative remedies with agencies including MeitY, MHA/I4C, RBI, SCI, PMO, and NCSC from 2022 to 2025 and receiving no investigative response, the Petitioner approaches this Court as a last recourse and in its constitutional capacity under Kesavananda Bharati v. State of Kerala (1973) AIR 1973 SC 1461.
2. Whether the systematic collection of a citizen's complete digital identity through consent obtained by fraudulent concealment of purpose — through Android app permissions, NBFC KYC collection, and adtech SDK surveillance — followed by permanent transfer of that identity to a foreign criminal infrastructure, constitutes a violation of the basic structure of the Constitution through destruction of digital constitutional personhood of 80 million Indian citizens under Article 21 as extended by Puttaswamy (2017) 10 SCC 1.
3. Whether the State's five-year decision to investigate only the financial dimension of this crime — attaching money, arresting call centre workers — while completely ignoring the data dimension — the 80 million stolen biometric records, the Chinese principal architects, and the adtech surveillance infrastructure — constitutes a single investigative mischaracterisation that converted a remediable harm into a permanent and irreversible constitutional injury — and whether that irreversible injury creates a continuing constitutional tort for which this Court as Constitutional Guardian must now provide structural remedy.
4. Whether India's failure for 14 years to invoke "Section 3(4) of the Extradition Act **1962** as inserted by Act 66 of **1993**"read with UNCAC Article 44 and UNTOC — both ratified by India in 2011 — against any named Chinese principal architect of this ecosystem, constitutes an arbitrary abdication of available legal power that violates Article 14 and has allowed the master custodian of 80 million Indian citizens' biometric records to remain permanently beyond legal reach.
5. None of these three questions have been raised, argued, or decided in SMW (Crl.) No. 3 of 2025 or any other pending matter. This petition is filed as a fresh, independent

constitutional case on these specific questions and must not be tagged to or clubbed with any existing matter without first examining whether these distinct constitutional questions are covered in that matter.

6. This matter requires prompt attention as an urgent case of national importance due to ongoing, not historical, harm—personal and financial data of Indian citizens are continuously compromised. The threat uses advanced technologies like AI automation, deepfake impersonation, and international data systems, which current proceedings do not address. Delays further expand the risk, making remedies less effective. This case is classified as **EXTREMELY URGENT** for two independent reasons:

- **i.** **PERSONAL LIBERTY —** 105 Indian citizens per hour are subjected to digital arrest, a form of coercive psychological detention without legal basis, enabled entirely by stolen biometric data — constituting hourly violations of Article 21.
- **ii.** **NATIONAL SECURITY —** 80 million complete biometric identity profiles of Indian citizens are held by a foreign criminal infrastructure and actively weaponised in real time.

7. 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. This is not a petition about what happened. It is a petition about what is happening right now — AND about the one wrong investigative decision made five years ago that made everything that followed IRREVERSIBLE. The State chose to follow the money. It should have followed the data. That choice cannot be undone. Its consequences can — and must — be addressed by this Court acting as Constitutional Guardian.

8. The irreversible consequence of one wrong investigative decision. In 2020, the State targeted money flows in the Chinese loan app ecosystem—freezing accounts, making arrests, and confiscating funds—while neglecting to investigate data. This choice led to permanent harm: while money and arrests can be reversed, exposed data cannot. An Aadhaar number in a foreign database, facial biometrics, exported contacts, or photos used in deepfake models are irreversible once leaked.

9. Five years of PMLA enforcement has produced Rs. 800 crores in attached funds — a finite, one-time result. Five years of ignoring the data has produced 80 million permanently compromised digital identities — an infinite, self-regenerating source of harm. In the AI era, each stolen record generates not one fraud but potentially hundreds

— through voice cloning, deepfake generation, automated mule account creation, and precision-targeted psychological manipulation. The State made one wrong investigative decision. This Court cannot undo that decision. But it can — and under the basic structure doctrine and Article 142, it MUST — ensure that the consequences of that wrong decision are remedied as completely as the law permits. That is the relief this petition seeks.

Gen	Method	Details
1	Play Store apps	data theft via permissions, banned
2	APK/WhatsApp distribution	same backend
3	NBFC license misuse	fake compliance
4	Telegram bots	direct KYC collection
5	AI automation	deepfakes, offshore, no trace

10. This Hon'ble Court may note the core asymmetry: monetary attachment (e.g., ₹800 crore under PMLA) is reversible, but mass data theft is not. Once 80 million Aadhaar, PAN, biometric, and bank records are exfiltrated, they cannot be undone and continue to multiply across global fraud networks. The only effective remedy—never sought—is court-directed diplomatic action for forensic destruction of the original database, alongside prosecution to deter re-exfiltration. Each day of inaction allows further misuse, expansion of stolen data, and irreversible harm to citizens' identity security. the traced evidence chain — each link documented .

11. The adtech layer (never investigated) This petition identifies a dimension of the cyber fraud ecosystem that has never been investigated by any Indian agency and has never been placed before any Indian court: the adtech surveillance layer and its role in enabling real-time victim profiling. When a victim of digital arrest fraud receives a call, the fraudster knows the victim's correct Aadhaar-linked address, family members' names, approximate bank balance, and — in documented cases **— that the victim is ALONE AT HOME, has a SIGNIFICANT BANK BALANCE, and has NOT RECEIVED CALLS FROM FAMILY** for several hours preceding the fraud call. This last category of knowledge cannot come from a static stolen KYC database. It requires real-time or recent behavioural data — location data showing the victim is at home; call log data showing no recent family contact; financial data showing current balance. This

is the signature of an ACTIVE SURVEILLANCE LAYER operating at the time of the crime — not merely a historical data leak.

12. The InMobi SDK (FTC Consent Order 2016, Case C-4530: covert WiFi geolocation tracking even when GPS is OFF, on 100 million devices including children) and the Silverpush SDK (FTC Warning Letters 2016: ultrasonic audio beacon technology triggering device microphone access for cross-device tracking) were embedded in HUNDREDS of Indian consumer applications — not just loan apps. Both were collecting continuous, real-time behavioural data. Not one Indian agency has investigated whether this adtech data contributed to the victim profiling that enables the targeting precision of Generation 4 and 5 digital arrest operations. MeitY has not opened a single inquiry under Section 43A IT Act 2000 against either company — eight years after the FTC publicly documented their covert surveillance of Indian users including children. *(Ref annexure P4-P5 pg. no 60-67)*

13. This is the second body of the crime. It operates invisibly, inside legitimate-looking consumer apps. It was never investigated. And because it was never investigated, the surveillance infrastructure that enables precision victim targeting continues to function — silently, continuously, in the background of the devices of millions of Indian citizens who never took a loan and never appear in any cybercrime statistic.

14. The legal bridge that was never crossed — section 3(4) extradition act read with uncac article 44. India has no bilateral extradition treaty with China. This is the reason the government has consistently offered for not pursuing extradition of any named Chinese accused. This reason is legally incorrect and has been legally incorrect since 1993.

15. Section 3(4) of the Extradition Act 1962, inserted by Act 66 of 1993 with effect from 18.12.1993, specifically provides that where no bilateral treaty exists, the Central Government MAY TREAT ANY MULTILATERAL CONVENTION to which both India and the foreign State are parties as the legal basis for extradition. India ratified the United Nations Convention Against Corruption (UNCAC) in 2011. China ratified UNCAC in 2006. UNCAC Article 44 specifically permits use of the Convention as the extradition basis between State Parties with no bilateral treaty. India also ratified the United Nations Convention Against Transnational Organized Crime (UNTOC) in 2011. China has ratified UNTOC. Two legal bridges exist. Both have existed since 2011. NEITHER HAS EVER BEEN USED to file even one extradition request against any named Chinese accused in this ecosystem.

F

16. The Enforcement Directorate — the very agency that arrested 103 Indian nationals and attached Rs. 800 crores — has a dedicated page on its own official website explaining UNCAC and India's obligations under it. The agency knows UNCAC exists. The tool is available. The request has NEVER been filed. This petition asks this Court to direct the government to answer — under oath — why not.

17. This petition invokes this Hon'ble Court not merely in its jurisdiction under Article 32 — though that jurisdiction is fully and necessarily engaged — but in its role as the Guardian of the Constitution under the basic structure doctrine established in Kesavananda Bharati v. State of Kerala (1973) AIR 1973 SC 1461 and reaffirmed in Minerva Mills Ltd. v. Union of India (1980) 3 SCC 625.

18. The basic structure elements engaged in this petition are: (a) **Dignity and liberty of the individual** — 80 million citizens' digital constitutional personhood permanently in hostile foreign hands; (b) **Rule of law** — the architect of the largest data theft in Indian history walks free while his workers are prosecuted; (c) **Equality before law** — money harm pursued, data harm ignored; Indian workers prosecuted, Chinese architects never extradited; (d) **Judicial review itself** — 80 million victims cannot individually access courts; only this Court's guardian jurisdiction can reach them; (e) **Welfare state** — in the digital age, protection of citizens' digital identity is a constitutional welfare obligation.

19. Article 142 is not supplementary but ESSENTIAL — because complete justice for 80 million citizens requires structural directions that reach the data (on foreign servers), the architects (in China), and the infrastructure (which reconstitutes every 48–72 hours). Ordinary mandamus cannot reach these targets. Only structural judicial directions under Article 142 — monitored by this Court on a continuing basis as in Vineet Narain v. Union of India (1998) 1 SCC 226 — can provide complete justice.

20. Under Article 141, this Court is asked to declare that the DIGITAL CONSTITUTIONAL PERSONHOOD of every Indian citizen — their biometric identity, personal data, financial identity, and digital communications taken together — is a fundamental constitutional asset protected under Article 21 as extended by Puttaswamy. This declaration will govern not just this case but every digital rights case in the AI era. That is the guardian function. That is what this petition invokes.

LIST OF DATES AND EVENT

Date	Event
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.
2016 (March)	FTC issues warning letters to 12 developers using Silverpush SDK: ultrasonic audio beacons triggering device microphones without disclosure.
2017–2019	400–600 Chinese-backed predatory loan apps active in India. Each harvests contacts, SMS, location, photos, call logs — zero legitimate lending purpose. Includes: CashBean, RupeeLend, CashMama, ZipLoan, Quick Rupee, MiCredit, LoanZone, RupeeGo, and hundreds more.
2019 (Dec)– 2020 (Mar)	COVID-19 lockdown. App installs multiply 4x. 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.
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.
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.
2021 (mid)	Jeffrey Zhu (Zhu Wei) departs India BEFORE Look Out Circular issued. Carries administrative access to master harvested database of 80M+ records. Section 3(4) of the Extradition Act 1962 as inserted by Act 66 of 1993 with effect from 18.12.1993, read with UNCAC Article 44, was available as a legal tool since 2011 and was NEVER invoked. He has never faced any court in any jurisdiction. As of March 2026, his confirmed location is unknown — itself a documented investigative failure over five years.
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.

Date	Event
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.
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.
2023 (Aug)	Digital Personal Data Protection Act, 2023 enacted. Creates Data Protection Board, breach notification, consent framework, Rs. 250 crore penalty per violation.
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.
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.
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.
March 2026	Filing of this Petition. Five years of documented State inaction on the DATA dimension of this ecosystem — as distinct from and additional to the financial enforcement dimension which is already before this Court in SMW (Crl.) No. 3 of 2025. That matter addresses digital arrest fraud through forged documents. This petition addresses the distinct and deeper questions of: (i) the three-layer data collection architecture; (ii) the adtech surveillance layer never investigated; (iii) Section 3(4) Extradition Act 1962 and UNCAC Article 44 never invoked; and (iv) the constitutional doctrine of Digital Constitutional Personhood. This petition is filed as a FRESH CONSTITUTIONAL CASE on questions not covered in any pending matter. Administrative remedy completely exhausted as documented in Annexures P-14 and P-15. Pg no 95-106

IN THE HON'BLE SUPREME COURT OF INDIA

WRIT PETITION (CRIMINAL) NO. _____/2026

PUBLIC INTEREST LITIGATION

UNDER ARTICLE 32 OF THE CONSTITUTION OF INDIA

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 – 110003.

Email: secy-miety@gov.in Phone: 011-24301851

2. Union of India

Through the Secretary, Ministry of Home Affairs, North Block, Central Secretariat, New Delhi – 110001. Email: secy-mha@nic.in Phone: 011-23092011

3. Directorate of Enforcement

Through the Director, Lok Nayak Bhawan, Khan Market, New Delhi – 110003.

Email: director@enforcementdirectorate.gov.in Phone: 011-24692000

...Respondents...All Contesting Respondents

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

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.

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 scam fraud (**Rs. 1.5 Lakhs crore** loss till 2026) 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. Five years of intelligence submissions by this Petitioner to 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.

The figures and harm indicators placed before this Hon’ble Court are derived from official data published by the Ministry of Home Affairs through the Indian Cyber Crime Coordination Centre (I4C) and placed before Parliament. The Petitioner has undertaken a structured analysis of such official data to present the scale and immediacy of harm in measurable terms.

The Petitioner respectfully submits that he is a direct victim of the ecosystem described herein and has, thereafter, undertaken continuous independent inquiry into its operational evolution — from earlier organised cyber fraud patterns,

including those associated with regions such as **Jamtara**, to the present form of "Scam" fraud. The Petitioner has also submitted phase-wise intelligence inputs and process-level observations to competent authorities, which remain unacted upon.

It is submitted that the present matter reflects an ongoing and escalating threat affecting citizens on a real-time basis, with no effective remedial mechanism currently operational. The material placed before this Hon'ble Court is capable of verification and may be demonstrated, if required, during hearing.

In these circumstances, the Petitioner respectfully submits that the present case raises issues of **urgent national importance**, involving continuing violation of fundamental rights under Articles 14 and 21 of the Constitution of India and requiring immediate judicial consideration.

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

interest, 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. 1.5 Lakh crore in losses till 2026, 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, PMO, and NCSC between 2022 and 2025. All submissions received standard acknowledgements or no response. Zero investigative action was triggered. Detailed are at Annexures P-14 and P-15 (Ref: pg. no 96-106). Administrative remedy is exhausted.

vi. Other Litigation: None pending.

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

viii. Similar Petition: "THAT THE PETITIONER HAS NOT FILED ANY OTHER PETITION EITHER BEFORE THIS COURT OR ANY OTHER COURT SEEKING SIMILAR RELEIF AS SOUGHT IN THE PRESENT WRIT PETITION.

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 National 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.**

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 40–47.)

2.2 That the Petitioner is a National Cyber Security Scholar who has formally submitted intelligence on this ecosystem to government bodies between 2022 and 2026, 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 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 Document 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) *Refer: page no 85-88*
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) *Refer: page no 85-88*
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) *Refer: page no 74-77*
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) *Refer: page no 64-67*

Permission Demanded	Any Legitimate Lending Purpose?	Actual Use Document in Evidence	Evidence Source
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
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 borrower 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 crossmatching with public records (Annexure P-11 *Refer: page no 85-88*).

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	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 3(4) (which does not require a treaty). Diplomatic silence towards China.

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
Liu Yang / 'Michael Yang'	Beneficial owner, PowerBank Digital Tech; oversaw operations of 3 app networks in India.	ED Prosecution Complaint 2023; Karnataka Police FIR (loan app network)	Issued	Applied	NONE FILED	Absconded to Shenzhen. Never prosecuted.	Same structural failure: LOC issued; no follow-through on extradition. No MLAT request to 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 3(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 notices 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	Deportation without prosecution = impunity by process. India voluntarily surrendered its only leverage — criminal prosecution —

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
						took no recorded action.	in exchange for nothing.
6 unnamed Chinese nationals	Operational call centre staff, Chinese loan app, Hyderabad.	Telangana Police FIR 2020	N/A — arrested	N/A	N/A	DEPORTED December 2020 without criminal conviction.	Same pattern: deport instead of prosecuting. Identity records 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.

Generation	Period	Method	State Response	Time to Reconstitute	What Continued Unchanged
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.
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 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 141 & 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 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)BRIEF DESCRIPTION OF ANNEXURES RELIED UPON

The following Annexures are filed in support of this Writ Petition and form an integral part thereof. Each Annexure is briefly described below with its start and end pagination in the Paper Book:

Annexure P-1 (Pages 48–52): Constitution of India — Articles 14, 19(1)(a), 21, 32, and 142, establishing the fundamental rights framework invoked in this Petition and this Hon'ble Court's jurisdiction under Article 32 to enforce fundamental rights and under Article 142 to pass orders for complete justice.

Annexure P-2 (Pages 53–56): Information Technology Act, 2000 — Sections 43A, 66, 69, 69A, 72, 72A along with Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, establishing the statutory framework for data protection and cyber offences that the Ministry of Electronics and Information Technology failed to exercise against InMobi and Silverpush for over eight years despite constructive notice from the US Federal Trade Commission.

Annexure P-3 (Pages 57–59): Digital Personal Data Protection Act, 2023 (Complete Text), enacted on 11th August 2023 but never operationalised — the Data Protection Board has not been

constituted and implementing Rules have not been notified as of date, rendering the statutory protections promised to 80 million affected citizens entirely inert.

Annexure P-4 (Pages 60–63): FTC Consent Order — In the Matter of InMobi Pte Ltd, June 2016 (Docket No. C-4530), evidencing that InMobi covertly tracked geolocation of approximately 100 million mobile devices including children's devices through WiFi scanning without consent, and was penalised USD 950,000 by the US regulator. India took zero enforcement action for 8+ years despite this being public record.

Annexure P-5 (Pages 64–67): FTC Staff Warning Letters to Developers Using Silverpush SDK, March 2016, evidencing that Silverpush's SDK utilised ultrasonic audio beacons to activate smartphone microphones for cross-device tracking without user disclosure. Silverpush Technologies Pvt Ltd is an Indian company headquartered in Delhi NCR, yet no Indian regulatory investigation was ever initiated.

Annexure P-6 (Pages 68–70): RBI Warning Circular — Unauthorised Digital Lending Apps (RBI/2020-21/116), dated 23rd December 2020, wherein the Reserve Bank of India formally acknowledged harm from unauthorised lending apps accessing mobile contacts and photographs. The Circular addressed only financial conduct and issued no direction regarding data already exfiltrated, data destruction, or notification to affected borrowers.

Annexure P-7 (Pages 71–73): RBI Digital Lending Guidelines, August 2022 (RBI/2022-23/111), the most comprehensive regulatory response to date, which regulates future digital lending

conduct but contains no provision for recovery, destruction, or remediation of personal data already exfiltrated during 2019–2022, thereby confirming the structural regulatory gap at the heart of this Petition.

Annexure P-8 (Pages 74–77): MHA I4C Annual Cyber Crime Data Reports 2022, 2023, and 2024, documenting that Rs. 2,140 crore was lost to digital arrest fraud in 2024 alone, 4.6 million complaints were registered on NCRP between 2019–2025, the recovery rate is approximately 28%, and the conviction rate is approximately 2.3% — quantifying both the scale of harm and the systemic inadequacy of enforcement.

Annexure P-9 (Pages 78–80): Parliamentary Standing Committee on Home Affairs — 237th Report, officially recording that the Indian Cyber Crime Coordination Centre (I4C) underspent approximately 34% of its allocated budget over three consecutive years, and documenting significant gaps in State police cyber cell capabilities and inter-State coordination — constituting Parliament's own acknowledgement of the institutional failures raised in this Petition.

Annexure P-10 (Pages 81–84): Enforcement Directorate Press Releases — Operation Hawk (April 2024) and Operation Chakra-II (CBI, August–September 2023), officially confirming 103 total arrests (all Indian nationals), Rs. 800+ crore in PMLA attachments, zero arrests of any Chinese national, zero extradition proceedings initiated, and zero data recovery actions — evidencing the selective money-only enforcement approach challenged in this Petition.

Annexure P-11 (Pages 85–88): Threat Intelligence Reports by CloudSEK and Group-IB India confirming circulation of 80 million+ Indian KYC records (Aadhaar, PAN, bank accounts, facial photographs, addresses, phone numbers) on dark web marketplaces at Rs. 500–2,000 per 1,000 records, traced to the loan app/NBFC data pipeline, with peak availability correlating precisely with the departure of Chinese principal architects in mid-2021.

Annexure P-12 (Pages 89–91): MEA Parliamentary Reply (December 2024) confirming that 5,200+ Indian nationals were trafficked to cyber fraud compounds in Myanmar and Southeast Asia between 2020–2024, of whom 3,100+ have been repatriated — the State acted to rescue enslaved workers but did not dismantle the data pipeline that funded and sustained those operations.

Annexure P-13 (Pages 92–94): NCRB "Crime in India" Reports 2022 and 2023 — Chapter on Cyber Crime, officially recording a conviction rate of approximately 2.3%, charge-sheeting rate of approximately 38%, and 78,940 pending trial cases — establishing that the ordinary criminal justice system is structurally incapable of providing effective remedy, thereby independently justifying this Court's exercise of jurisdiction under Article 32.

Annexure P-14 (Pages 95–100): Petitioner's Representations to Government Authorities — MeitY, RBI, MHA/I4C, Supreme Court of India, PMO, and NCSC (2022–2025) along with Proof of Delivery (Speed Post receipts, portal acknowledgements, email records), establishing exhaustion of administrative remedies and documenting that specific, expert intelligence was submitted to six government bodies with no investigative response.

Annexure P-15 (Pages 101–106): Petitioner's Cyber Security Intelligence Submissions and Research Documents, comprising technical analysis of the three-layer data harvesting pipeline, Chinese operator corporate footprint through ROC filings, dark web KYC data evidence, InMobi/Silverpush SDK analysis, and the five-generation threat evolution pattern — establishing that the representations were actionable expert intelligence, not general complaints.

Annexure P-16 (Pages 107–111): Prevention of Money Laundering Act, 2002 — Sections 5, 8, 17, along with Extradition Act, 1962 (as amended by Act 66 of 1993) — Section 3(4), establishing that statutory mechanisms exist for treating exfiltrated data as proceeds of crime and for initiating extradition without a formal treaty — both available tools that have never been used against any Chinese national accused in the digital dacoity ecosystem.

Annexure P-17 (Pages 112–113): Credential and Certificate for Subject Matter Expert — confirming the Petitioner's status as a National Cyber Security Scholar under the NSD program at Rashtriya Raksha University, an institution established by the Ministry of Home Affairs, establishing the Petitioner's domain expertise and bona fide standing to present technical arguments in this matter.

b) <u>Violation of Article 21 — Three-Layer Data Theft as Continuing Privacy Violation</u>

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.

c) <u>Violation of Article 21 — Right to Life: Weaponised Data Causing Deaths</u>

That the weaponisation of stolen biometric data to perpetrate (a) digital arrest fraud — Rs. 1.5Lkahs crore extracted till 2026, 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.

d) 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).

e) 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.

f) 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.

g) 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 3(4) proceedings, and UNCAC cooperation, the return or verified forensic destruction of this data. This obligation has never been discharged.

h) Failure to Operationalise DPDPA 2023 — Abdication of Statutory Duty

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.

i) Structural Failure: App-Level Enforcement Cannot Stop Infrastructure-Level Crime

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.

j) 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 3(4) to extradite without a treaty. In each case it omitted to act. Each omission, documented in this Petition, is a constitutional tort.

5. GROUND FOR INTERIM RELIEFS

The Petitioner respectfully submits the following grounds in support of the prayer for interim relief, demonstrating that the balance of convenience favours the grant of interim directions and that irreparable harm will result if interim directions are not granted:

(a) GROUND — EXTRADITION ACCOUNTABILITY: Section 3(4) of the Extradition Act 1962 as inserted by Act 66 of 1993 read with UNCAC Article 44 was never invoked against any named Chinese accused notwithstanding its availability as a legal tool since 2011. Jeffrey Zhu (Zhu Wei), the principal architect of the data exfiltration ecosystem, departed India before a Look Out Circular was issued. Each day of non-invocation causes continuing and irreversible harm.

(b) GROUND — DATA ACCOUNTABILITY: The State has never treated citizen data as a distinct forensic investigation target. No government agency has, to the Petitioner's knowledge, filed any proceeding for data recovery or destruction with respect to the 80 million+ Indian citizen records documented in dark web circulation since 2021. The absence of any data-directed inquiry constitutes a continuing constitutional failure under Article 21.

(c) GROUND — ROOT CAUSE ANALYSIS MISSING: The documented Root Cause Analysis underlying existing Government SOPs — Mule AI Hunter, Telecom SOP, CNAP, and I4C 1930 — has never been placed on record to demonstrate whether the three-layer data collection architecture (Android permissions exploitation, shell NBFC KYC collection, adtech SDK surveillance) was identified as the proximate cause enabling digital arrest fraud. Without Court intervention, this factual gap will remain undisclosed.

(d) GROUND — VICTIM PROFILING MECHANISM UNINVESTIGATED: Digital arrest fraudsters have demonstrated knowledge of victims' location, bank balance, and absence of recent family contact at the precise time of the fraud call — targeting intelligence that exceeds what a static KYC database can provide and is consistent with an active real-time surveillance layer. No agency has investigated this profiling mechanism. The continuing operation of this layer causes hourly harm to Indian citizens.

(e) GROUND — ADTECH SURVEILLANCE UNINVESTIGATED: InMobi Technologies Pvt Ltd was subject to an FTC Consent Order (Case C-4530, 2016) for covert WiFi geolocation tracking of 100 million devices including children. Silverpush Technologies Pvt Ltd was subject to FTC Warning Letters (2016) for ultrasonic audio beacon SDK technology. MeitY has not opened any inquiry under Section 43A IT Act 2000 against either entity in eight years. The adtech surveillance infrastructure continues to operate in Indian consumer applications.

(f) GROUND — ABSCONDERS UNACCOUNTED: For each named Chinese accused (Zhu Wei, Liu Yang, Zhuang Wei, Wang Xin, Chen Wei), the dates of Look Out Circulars and whether each LOC was issued before or after each accused's departure from India are not on public record. No extradition request has been filed against any of these accused. Their continued impunity constitutes a continuing violation of Article 14.

(g) GROUND — URGENCY AND IRREVERSIBILITY: According to official I4C/MHA data, 105 Indian citizens per hour receive digital arrest calls enabled by stolen biometric data, and Rs. 8.5 crore is coercively transferred per hour. Unlike monetary harm, data harm is irreversible — once biometric and identity records are in criminal hands, they generate an

unlimited stream of AI-personalised fraud operations. Every day without judicial intervention increases the quantum of irreversible harm.

6. 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 (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 "under **Section 3(4)** of the Extradition Act, 1962 as inserted by Act 66 of 1993"— 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: "under **Section 3(4)** of the Extradition Act, 1962 as inserted by Act 66 of 1993"; Art. 21 (continuing harm from absconding accused); Art. 14 (discriminatory impunity); Vineet Narain v. UOI (1998) — Court-monitored investigation.*

(c) COURT-DIRECTED SIT INVESTIGATION INTO DATA PIPELINE

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 (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) 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).

(k) 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.

(l) RECOGNITION OF CONSTITUTIONAL TORT

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 'Tort' against the people of India, warranting judicial supervision until fully remedied.

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

(m) 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.

7. PRAYER FOR INTERIM RELIEFS

Pending final disposal of this Petition, the Petitioner most humbly prays that this Hon'ble Court may be pleased to direct the Respondents to file sworn affidavits on the following:

(a) EXTRADITION AFFIDAVIT Direct Respondents No. 1 and 2 to file an affidavit within two weeks disclosing: (i) whether Section 3(4) of the

Extradition Act 1962 read with UNCAC Article 44 was ever invoked against any named Chinese accused; (ii) if not — the name of the officer who decided against invocation and the written reasons recorded in the file; and (iii) the confirmed current location of Zhu Wei (alias Jeffrey Zhu) and whether the Look Out Circular against him was issued before or after his departure from India.

(b) DATA AFFIDAVIT Direct Respondents No. 2 and 3 to file an affidavit within two weeks disclosing: (i) whether any seized citizen data from the Chinese loan app ecosystem is in any government agency's custody; (ii) if yes — why no notification was given to affected citizens; (iii) if no — why citizen data was never treated as a distinct forensic investigation target separate from money flows; and (iv) whether any court has ever been petitioned for a data destruction order against exfiltrated Indian citizen data held on foreign servers.

(c) ROOT CAUSE AFFIDAVIT Direct Respondent No. 2 to file an affidavit within three weeks disclosing: (i) the documented Root Cause Analysis underlying existing SOPs — Mule AI Hunter, Telecom SOP, CNAP, and I4C 1930; and (ii) whether any such analysis identified the three-layer data architecture — Android permissions, shell NBFC KYC collection, and adtech SDK surveillance — as the proximate cause enabling digital arrest fraud.

(d) VICTIM PROFILING AFFIDAVIT Direct Respondent No. 2 to file an affidavit within three weeks disclosing: (i) in documented digital arrest cases, how fraudsters knew the victim was alone, had a significant balance, and had no recent family calls — targeting intelligence that exceeds what a static KYC database can provide; and (ii) whether any agency

investigated whether InMobi or Silverpush SDK data contributed to this real-time targeting capability.

(e) ADTECH AFFIDAVIT Direct Respondent No. 1 to file an affidavit within two weeks disclosing: (i) whether any inquiry or penalty proceeding was ever initiated against InMobi Technologies Pvt Ltd or Silverpush Technologies Pvt Ltd under Section 43A of the IT Act 2000 in respect of the conduct documented in the FTC Consent Order (Docket No. C-4530, 2016) and FTC Warning Letters (March 2016); and (ii) if not — the specific reasons for eight years of inaction on documented covert surveillance of Indian users including children.

(f) ABSCONDERS STATUS AFFIDAVIT Direct Respondents No. 2 and 3 to file a complete status report within two weeks in respect of each named Chinese accused — Zhu Wei, Liu Yang, Zhuang Wei, Wang Xin, and Chen Wei — disclosing for each: (i) date of Look Out Circular and whether issued before or after departure; (ii) current confirmed location; (iii) whether any formal extradition request was ever filed; and (iv) whether any Red Corner Notice has been successfully processed by Interpol.

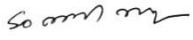
8. VERIFICATION

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-17 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

DRAWN ON: 25-03-2026

FILED BY:



Nitish Kumar

Petitioner-in-Person

Phone: +91-9082843142

PUBLIC INTEREST LITIGATION (PIL)

IN THE SUPREME COURT OF INDIA

EXTRA ORDINARY WRIT JURISDICTION

WP (Criminal) NO. _____ OF 2026

In the Matter of

"Nitish Kumar v. Union of India & Ors."

AFFIDAVIT

I, **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 do hereby solemnly affirm and declare hereby as under:

1. That I am the Petitioner-in-person in the aforesaid Writ Petition (Criminal) PIL No. Of 2026 and well aware of the facts and circumstances of the case and competent to swear this affidavit for self.

2. That the contents of the Instant Writ petition PIL from page no 1 to 37 in paras 1 to 8 and synopsis and list of dates from page B to H an accompanying

NOTARY SURINDER KUMARI SHARMA Regn. No.14935 Valid Upto:20.09.2029 S.A.S. Nagar (Mohali) Pb. GOVT. OF INDIA

9/4/26

ATTESTED

SURINDER KUMARI SHARMA
Notary, S.A.S. Nagar (Mohali)

applications(s) are true to my personal knowledge and belief and that no material facts have been concealed therefrom.

3. That the Annexures are True/Translated Copies of their respective originals.

4. That there is no personal interest, personal gain, private motive or any other oblique reason in filing this PIL by the petitioner. No Civil,Criminal or Revenue litigation is filed by or pending against the petitioner which could have a legal nexus with the present petition.

5. That the petitioner has approached the concerned authority vide Annexure(s) P 1 to P16 and no reply has been received till date.

DEPONENT

VERIFICATION:-

I, the above-named deponent hereby declare that the contents of the affidavit are true and correct to the best of my knowledge and belief and that no material facts or detail has been concealed therefrom.

Verified at Kharar on 09th April 2026

NOTARY SURINDER KUMARI SHARMA Regn. No.14935 Valid Upto:20.09.2029 S.A.S. Nagar (Mohali) Pb. GOVT. OF INDIA

ATTESTED

SURINDER KUMARI SHARMA
Notary, S.A.S. Nagar (Mohali)
9/4/26

DEPONENT

Adhaar No - 7538-5941-9077

Certified that the Affidavit/GPA/SPA/ I.Bond has been readover & explained to the Deponent/Executant who seemed perfectly to understand the same at the time of making thereof.
I identified the deponent/executant who sign./thumb marked in my presence.

The contents of this Affidavit/Document has been explained to the deponent/executants. He/She has admitted the same to be correct. The deponent/executant has signed Register at Sr. No. 631 P. No. 58 Date. 9/4/26

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.

Provision / Case	Bare Text / Principle	Application in This Petition
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.
Section 3(4) of the Extradition Act **1962** as inserted by Act 66 of 1993	Extradition with and without formal treaty (reciprocal basis).	No treaty with China required for Section 3(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.
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.

Provision / Case	Bare Text / Principle	Application in This Petition
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.

MASTER ANNEXURE INDEX

Each row traces one piece of evidence from its original source to the specific constitutional violation it proves in the Petition.

Annexure	Document	Fact Proved	Petition Para	Constitutional Provision Engaged	Verifiable Source
P-1	Constitution of India — Arts. 14, 19(1)(a), 21, 32, 142	Fundamental rights violated; Court's jurisdiction to grant relief; power to pass complete justice orders.	Questions of Law (a)–(i); Grounds (a)–(i)	Arts. 14, 19(1)(a), 21, 32, 142 directly	indiacode.nic.in
P-2	IT Act 2000 (Ss. 43A, 66, 69, 72A) + IT Rules 2011	State's statutory power to mandate data protection and penalise covert data collection — power not exercised for 8+ years against InMobi/Silverpush.	Para 2.3.4; Ground (d); Prayer (e)	Art. 14 (arbitrary non-exercise of statutory power)	indiacode.nic.in; meity.gov.in
P-3	Digital Personal Data Protection Act, 2023	Parliament enacted a specific law to protect citizens' data rights in August 2023. Board never constituted. Rules never notified. Effective protection: ZERO.	Para 2.7.1(f); Ground (g); Prayer (g)	Art. 21 (statutory right enacted but unenforceable); Mandamus ground crystallised	Gazette of India, 11 Aug 2023; meity.gov.in
P-4	FTC Consent Order — InMobi, June 2016 (Case C-4530)	InMobi covertly tracked 100M devices including children via WiFi without consent. USD 950,000 penalty. US regulator acted in 2016. India: zero action for 8+ years.	Para 2.3.4, 2.6; Ground (d); Prayer (e)	Art. 14 (8 years of arbitrary inaction on documented foreign regulatory finding)	ftc.gov/legal-library/cases/152-3116-inmobi
P-5	FTC Warning Letters — Silverpush SDK, March 2016	Silverpush SDK triggered device microphones via ultrasonic audio beacons without disclosure. US regulator warned developers in 2016. India: zero investigation.	Para 2.3.4, 2.6; Ground (d); Prayer (e)	Art. 14 and Art. 19(1)(a) — covert microphone access is surveillance	ftc.gov — search 'Silverpush warning letters March 2016'
P-6	RBI Warning Circular RBI/2020-21/116 (2021)	RBI itself acknowledged unauthorized digital lending apps causing harm from 2021. Yet: no data-specific action, no destruction order, no	Para 2.7.1; List of Dates 2021 row	Art. 14 (State aware of harm from 2021; no data remedy in 5 subsequent years)	rbi.org.in — Circular RBI/2020-21/116

Annexure	Document	Fact Proved	Petition Para	Constitutional Provision Engaged	Verifiable Source
		NBFC audit of data storage practices.			
P-7	RBI Digital Lending Guidelines, August 2022	Forward-looking regulation issued in 2022 — does not address retrospective data already exfiltrated. No data destruction provision. Confirms State knew of problem but chose money-only remedy.	Para 2.7.1; List of Dates 2022 row	Art. 14 — retrospective data harm not addressed	rbi.org.in — RBI/2022-23/111
P-8	MHA I4C Annual Cyber Crime Data Reports 2022–2024	Official State data: Rs. 2,140 crore lost to digital arrest in 2024; 4.6M total complaints; 28% recovery rate; 2.3% conviction rate. Every digital arrest call uses stolen Aadhaar data.	Para 2.1, 2.12; Synopsis Harm Clock; Ground (b)	Art. 21 (Rs. 2,140 crore harm directly traceable to exfiltrated data); Art. 14 (2.3% conviction = systemic denial of justice)	cybercrime.gov.in; MHA press releases; Parliamentary Q&A
P-9	Parliamentary Standing Committee — 237th Report	Parliament's own committee found I4C budget underspent 34% over 3 years; systemic coordination failure. State failure is not disputed — it is officially recorded.	Para 2.7.1; List of Dates 2022 row	Art. 14 — official parliamentary record of systemic failure	loksabha.nic.in — Committee Reports section
P-10	ED Press Releases: Operation Hawk (2024), Chakra-II (2023)	Official confirmation of 103 total arrests — every one an Indian national at operational level. Zero Chinese nationals prosecuted. Rs. 800 crore attached. Zero data recovery.	Para 2.5, 2.7.1; Ground (c), (d); Prayer (a), (b)	Art. 14 — discriminatory prosecution; data ignored while money attached	enforcementdirectorate.gov.in — Press Releases
P-11	CloudSEK + Group-IB India Reports — 80M KYC Data	Independent threat intelligence confirming 80M+ Indian KYC records (Aadhaar, PAN, bank, face, address, phone) in dark web circulation from loan app pipeline. Price: Rs. 500–2,000 per 1,000 records.	Para 2.4, 2.7.1; Ground (a); Synopsis para 6	Art. 21 (documented scale of biometric data breach); Art. 14 (State notified; no action)	cloudsek.com/blog; Group-IB India public reports
P-12	MEA Parliamentary Reply —	Official confirmation that 5,200+ Indians trafficked to SE Asia for	Para 2.1; List of Dates; Supporting	Art. 21 (State's duty to protect citizens from	Lok Sabha / Rajya Sabha starred questions; mea.gov.in

Annexure	Document	Fact Proved	Petition Para	Constitutional Provision Engaged	Verifiable Source
	Myanmar Repatriation	cyber fraud compounds; 3,100+ repatriated. Cyber slavery documented at highest government level.	context for scale of harm	cyber slavery); Art. 14 (systemic trafficking enabled by same data ecosystem)	
P-13	NCRB Crime in India 2022, 2023 — Cyber Crime Chapter	Official statistics: cyber crime conviction rate 2.3%; financial fraud = 67% of all cyber complaints. Proves that the judicial system is structurally incapable of providing effective remedy — making Supreme Court intervention necessary.	Para 2.12; Maintainability section 1B	Art. 14 (2.3% conviction = denial of equal justice); Art. 32 (Supreme Court intervention necessary where ordinary remedy is structurally unavailable)	ncrb.gov.in — annual reports
P-14	Petitioner's Representations to Government Authorities (2022–2025)	Proof that intelligence was submitted to MeitY, MHA, RBI, TRAI, PMO, and NCSC. Proof that no investigative action was taken. Establishes exhaustion of administrative remedy and makes State's inaction into a documented constitutional omission.	Para 2.13; PIL Guidelines para (v); Ground (i); Prayer (f)	Art. 32 (administrative remedy exhausted; Supreme Court jurisdiction engaged)	Petitioner's personal records — compile all delivery proofs
P-15	Petitioner's Cyber Security Intelligence Submissions	Technical intelligence submitted to government specifically identifying the Chinese data harvesting pipeline, Jeffrey Zhu corporate footprint, 80M KYC dark web circulation, and InMobi/Silverpush SDK deployment. Proves that the State had specific expert evidence and chose not to act.	Para 2.13; Ground (i); Prayer (f)	Art. 14 (arbitrary non-action on specific, expert, documented intelligence); Art. 21 (harm continued after State was specifically warned)	Petitioner's personal records — compile research documents and submissions
P-16	PMLA 2002 (Ss. 5, 8, 17) + Extradition Act 1962 (Ss. 3, 4)	Statutory basis showing: (a) PMLA Section 8 allows court-ordered confiscation/destruction	Para 2.5, 2.7.1; Ground (f); Prayer (b)	Art. 14 (Extradition Act Section 3(4) available and never used	indiacode.nic.in; Ministry of Law & Justice

Annexure	Document	Fact Proved	Petition Para	Constitutional Provision Engaged	Verifiable Source
		— applicable to data as proceeds/instrument of crime; (b) Extradition Act Section 3(4) allows extradition without formal treaty on reciprocal basis — never invoked for any Chinese accused.		= arbitrary omission)	

ANNEXURE P-1

Document Title:

Constitution of India — Articles 14, 19(1)(a), 21, 32, and 142

Source Authority:

Ministry of Law & Justice, Government of India (Official Gazette; India Code)

Document Date:

Constitution of India, 1950 (as amended to date)

Source / URL:

https://indiacode.nic.in/handle/123456789/1362

Also available at: https://legislative.gov.in

Petition Paragraph Reference:

Questions of Law (a) through (i); Grounds (a) through (i); Prayer Nos. (a) through (o)

Fact Proved by This Document:

This document establishes the fundamental rights forming the basis of the present Petition, including equality before law, freedom of speech and expression, and protection of life and personal liberty. It further affirms the jurisdiction of this Hon'ble Court under Article 32 to enforce these rights, along with the plenary powers under Article 142 to pass such orders as may be necessary to do complete justice.

EXTRACTED TEXT — ARTICLES RELIED UPON

ARTICLE 14 — EQUALITY BEFORE LAW

> *"The State shall not deny to any person equality before the law or the equal protection of the laws within the territory of India."*

Judicial Expansion (to be read with this Article):

E.P. Royappa v. State of Tamil Nadu (1974) 4 SCC 3: 'Equality is a dynamic concept with many aspects and dimensions and it cannot be cribbed, cabined and confined within traditional and doctrinaire limits... Arbitrariness is antithetical to the rule of law... Where an act is arbitrary, it is implicit in it that it is unequal both according to political logic and constitutional law and is therefore violative of Article 14.' [Applied in this Petition to establish that the State's arbitrary discrimination between money harm (pursued) and data harm (ignored), and between Indian accused (prosecuted) and Chinese principals (never extradited), violates Article 14.]

ARTICLE 19(1)(a) — FREEDOM OF SPEECH AND EXPRESSION

"All citizens shall have the right to freedom of speech and expression."

Judicial Expansion:

Shreya Singhal v. Union of India (2015) 5 SCC 1: The Court struck down Section 66A of the IT Act recognising that the right of free expression includes the right to communicate in digital spaces without ambient fear of surveillance or coercion. [Applied in this Petition: when 80 million citizens' devices have been comphands;ively Surveilled and their data is in criminal hands, the ambient fear this creates constitutes an unconstitutional chilling effect on digital expression.]

People's Union for Criminal Liberties v. Union of India (1997) 1 SCC 301: Telephone tapping without lawful authority violates the right to privacy implicit in Article 21 and the right to expression under Article 19(1)(a). [Applied: SDK-based audio and SMS surveillance is equivalent.]

ARTICLE 21 — PROTECTION OF LIFE AND PERSONAL LIBERTY

"No person shall be deprived of his life or personal liberty except according to procedure established by law."

Judicial Expansion:

Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1 (Nine-Judge Constitutional Bench): RIGHT TO PRIVACY IS A FUNDAMENTAL RIGHT under Article 21. The judgment holds at para 643 (Chandrachud J.): 'The right to privacy includes at its core the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home and sexual orientation. Privacy also connotes a right to be left alone. Privacy safeguards individual autonomy and recognises the ability of the individual to control vital aspects of his or her life. Personal choices governing a way of life are intrinsic to privacy. Privacy protects heterogeneity and recognises the plurality and diversity of our society.' The judgment further holds that informational privacy and data autonomy — the right to control information about oneself — is a core component of the right to privacy under Article 21. [PRIMARY AUTHORITY in this Petition. The triple test of legality, legitimate aim, and proportionality applies to any interference with privacy.]

Paschim Banga Khet Mazdoor Samity v. State of W.B. (1996) 4 SCC 37: 'Article 21 imposes an obligation on the State to safeguard the right to life of every person... Failure on the part of a Government hospital to provide timely medical treatment to a person in need of such treatment results in violation of his right to life guaranteed under Article 21.' [Applied by analogy: failure of the State to protect citizens from documented, systematic harm to life and dignity violates Article 21.]

Nilabati Behera v. State of Orissa (1993) 2 SCC 746: Sovereign immunity cannot shield the State from constitutional tort liability. Compensation is payable for violation of fundamental rights by the State. [Applied: State's documented omissions causing 83+ deaths and Rs. 2,140 crore in harm = constitutional tort.]

ARTICLE 32 — REMEDIES FOR ENFORCEMENT OF RIGHTS

"(1) The right to move the Supreme Court by appropriate proceedings for the enforcement of the rights conferred by this Part is guaranteed. (2) The Supreme Court shall have power to issue directions or orders or writs, including writs in the nature of habeas corpus, mandamus, prohibition, quo warranto and certiorari, whichever may be appropriate, for the enforcement of any of the rights conferred by this Part."

Dr. B.R. Ambedkar in the Constituent Assembly called Article 32 'the heart and soul of the Constitution.' Bandhua Mukti Morcha v. Union of India (1984) 3 SCC 161 established the Public Interest Litigation jurisdiction of this Court.

ARTICLE 142 — ENFORCEMENT OF DECREES AND ORDERS OF SUPREME COURT

"The Supreme Court in the exercise of its jurisdiction may pass such decree or make such order as is necessary for doing complete justice in any cause or matter pending before it."

This provision empowers this Court to issue structural directions — including directions binding on the Executive, directions to frame rules, and directions transcending ordinary mandamus — when necessary for complete justice. Applied in this Petition to support the structural injunction against pattern reconstitution (Prayer i) and the data recovery mandate (Prayer a).

TRUE COPY ANNEXURE P-1

I, Nitish Kumar, Petitioner-in-Person in W.P. (Criminal) No. _____ of 2026, do hereby certify that the document(s) annexed herewith as Annexure P-1 are TRUE COPIES of the original(s) / true copies of documents obtained from the public sources identified above. Each page is initialled by the Petitioner. This document is filed as evidence in support of the Writ Petition and is subject to verification by this Hon'ble Court.

Nitish Kumar
Petitioner-in-Person

Date: 25-03-2026

ANNEXURE P-2

Document Title:

Information Technology Act, 2000 — Sections 43A, 66, 69, 69A, 72, 72A along with Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

Source Authority:

Ministry of Electronics and Information Technology (MeitY), Government of India

Document Date:

IT Act: June 9, 2000 (as amended to date)

Section 43A inserted by IT (Amendment) Act, 2008

IT Rules: April 11, 2011

Source / URL:

https://indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf

https://meity.gov.in/content/security-privacy-and-cyber-laws

Petition Paragraph Reference:

Para 2.3.4 (Adtech SDK surveillance); Ground (d) (Article 14 — arbitrary non-exercise of statutory power); Prayer (e) (InMobi/Silverpush enforcement)

Specific Fact Proved by This Document:

This document establishes that the statutory framework under the Information Technology Act, 2000 and the 2011 Rules empowered the Ministry of Electronics and Information Technology to regulate, investigate, and penalize unauthorized or unlawful data collection practices. It demonstrates that such enforcement powers existed at least since 2011 in relation to entities such as InMobi and Silverpush engaged in covert data collection. The continued non-exercise of these statutory powers, despite the availability of legal mechanisms, constitutes arbitrary inaction and is violative of Article 14 of the Constitution of India.

KEY STATUTORY PROVISIONS — EXTRACTED TEXT

Section 43A — Compensation for Failure to Protect Data

"Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected."

EVIDENCE POINT: The FTC Consent Order (Annexure P-4) establishes that InMobi covertly tracked 100 million devices through WiFi data collection. This constitutes 'failure to implement reasonable security practices' within the meaning of Section 43A. InMobi's SDK was embedded in hundreds of Indian applications. Section 43A provides a direct cause of action against InMobi in India that MeitY has never exercised.

Section 66 — Computer Related Offences

"If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment of either description for a term which may extend to three years or with fine which may extend to five lakh rupees or with both."

EVIDENCE POINT: The unauthorised collection and transmission of device data — contacts, SMS, location, photographs — by Chinese loan app operators constitutes an offence under Section 66. FIRs invoking this Section have been filed in some cases, but the Section has never been applied to the SDK operators (InMobi, Silverpush) whose SDKs enabled part of this collection.

Section 69A — Power to Issue Directions for Blocking

"Where the Central Government or any of its officers specially authorised by it... is satisfied that it is necessary or expedient... in the interest of sovereignty

and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order... it may... direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource."

EVIDENCE POINT: This is the provision used to ban 59 Chinese apps in 2020. However, it was applied to user-facing app interfaces only — not to the SDK components performing data collection within non-banned apps, and not to the C2 server endpoints receiving the exfiltrated data. The Petition argues this incomplete application of Section 69A is arbitrary under Article 14.

Section 72A — Punishment for Disclosure of Information in Breach of Lawful Contract

"Save as otherwise provided in this Act or any other law for the time being in force, any person... who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punishable with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both."

EVIDENCE POINT: Shell NBFCs collected KYC data under the pretence of a regulated lending contract and disclosed it to Chinese-controlled servers — a clear Section 72A offence. This section has not been invoked in any case involving the NBFC KYC pipeline, to the Petitioner's knowledge.

IT (Reasonable Security Practices) Rules, 2011 — Rules 3, 4, 5, 6

Rule 3 defines 'sensitive personal data or information' to include passwords, financial information, physical/physiological/mental health conditions, sexual

orientation, medical records, and 'biometric information'. Aadhaar biometrics, PAN numbers, and facial photographs collected by loan apps all fall within this definition.

Rule 4 requires everybody corporate to publish a privacy policy disclosing the type of information collected, its purpose, means of collection, and the fact that it will not be shared with third parties without consent.

Rule 5 requires prior consent for collection of sensitive personal data and limits collection to what is necessary for the stated purpose.

EVIDENCE POINT: Every Chinese loan app that collected contacts, SMS, photographs, and location data in addition to credit-assessment information violated Rules 4, 5, and 6 of the IT Rules 2011 — rules that existed and were enforceable from 2011 onward. MeitY had full power to investigate and penalise from 2011. It did not act until 2021, and even then, never specifically investigated SDK-level data collection.

TRUE COPY — ANNEXURE P-2

I, Nitish Kumar, Petitioner-in-Person in W.P. (Criminal) No. _____ of 2026, do hereby certify that the document(s) annexed herewith as Annexure P-2 are TRUE COPIES of the original(s) / true copies of documents obtained from the public sources identified above. Each page is initialled by the Petitioner. This document is filed as evidence in support of the Writ Petition and is subject to verification by this Hon'ble Court.

Nitish Kumar
Petitioner-in-Person

Date: 25-03-2026

ANNEXURE P-3

Document Title:

Digital Personal Data Protection Act, 2023 (Complete Text)

Source Authority:

Ministry of Electronics and Information Technology (MeitY), Government of India — Gazette of India

Document Date:

Gazette of India Notification, August 11, 2023

Act No. 22 of 2023

Source / URL:

https://gazette.india.gov.in (search: Digital Personal Data Protection Act, 2023)

https://meity.gov.in/data-protection-framework

Petition Paragraph Reference:

Para 2.7.1(f); Ground (g); Prayer (g) — Mandamus for constitution of Data Protection Board and notification of Rules

Specific Fact Proved by This Document:

This document establishes that Parliament enacted the Digital Personal Data Protection Act, 2023 to protect the personal data of citizens and to create a statutory enforcement mechanism, including the establishment of the Data Protection Board of India. It demonstrates that, despite the enactment of the law, the enforcement framework—specifically the constitution of the Data Protection Board and the notification of necessary rules—has not been operationalized. This non-discharge of a statutory obligation renders the inaction amenable to judicial review and justifies the issuance of a writ of mandamus by this Hon'ble Court.

KEY PROVISIONS — EXTRACTED AND ANNOTATED

Section	Title	Statutory Obligation Created	Status as of March 2026 (Evidence of Non-Compliance)
Section 6	Consent	Personal data may only be processed for a specific lawful purpose with the consent of the data principal. Consent must be free, specific, informed, unconditional and unambiguous.	NEVER OPERATIONALISED. No consent standard has been enforced against any loan app or SDK operator. The 80 million records collected without consent were never subject to this provision because no Board exists to enforce it.
Section 8	Obligations of Data Fiduciary — Breach Notification	Data fiduciary must notify the Data Protection Board and each affected data principal in case of a personal data breach 'in such form and manner as may be prescribed' — within 72 hours under draft rules.	NEVER OPERATIONALISED. The CoWIN breach (2023), the loan app KYC pipeline breach (2020–22), and the IRCTC breach (2022) — none of these resulted in any notification to affected citizens under this provision because no Board and no prescribed form exist.
Section 18	Data Protection Board of India	Central Government to establish the Data Protection Board of India, appoint Chairperson and Members, establish headquarters, and provide for its functioning.	BOARD NEVER CONSTITUTED as of March 2026 — more than 2 years after enactment. This is the specific omission targeted by Prayer (g) of the Petition.
Section 33	Financial Penalties	Penalties for breach of obligations — up to Rs. 250 crore per violation (S. 33(1)); up to Rs. 200 crore for	NO PENALTY EVER LEVIED under this Act because no Board exists to levy them. InMobi and Silverpush — whose FTC-documented violations clearly

Section	Title	Statutory Obligation Created	Status as of March 2026 (Evidence of Non-Compliance)
		failure to notify breach (S. 33(2)); up to Rs. 10,000 per day for continuing violations.	engage these provisions — have never been investigated under DPDPA.
Section 40	Power to Make Rules	Central Government to notify rules within prescribed period after enactment.	RULES NOT NOTIFIED as of March 2026. Without rules, Sections 6, 8, and 18 cannot be operationalised. The Act sits enacted but entirely inert.

MANDAMUS GROUND: The non-constitution of the Data Protection Board and non-notification of implementing rules, more than 2 years after the DPDPA's enactment, is a specific, documented, provable abdication of statutory duty. Unlike a policy discretion, this is a ministerial duty — 'shall establish' is mandatory language. The Petitioner submits that this Court should issue a Writ of Mandamus with a specific 60-day compliance deadline for Board constitution and 90-day deadline for rule notification.

TRUE COPY — ANNEXURE P-3

I, Nitish Kumar, Petitioner-in-Person in W.P. (Criminal) No. _____ of 2026, do hereby certify that the document(s) annexed herewith as Annexure P-3 are TRUE COPIES of the original(s) / true copies of documents obtained from the public sources identified above. Each page is initialled by the Petitioner. This document is filed as evidence in support of the Writ Petition and is subject to verification by this Hon'ble Court.

Nitish Kumar
Petitioner-in-Person

Date: 25-03-2026

ANNEXURE P-4

Document Title:

FTC Consent Order — *In the Matter of InMobi Pte Ltd*, June 2016

Source Authority:

United States Federal Trade Commission (FTC) — Docket No. C-4530 / File No. 152-3116

Document Date:

FTC Consent Order finalized and published: June 22, 2016

Consent Agreement signed by InMobi Pte Ltd

Source / URL:

https://www.ftc.gov/legal-library/browse/cases-proceedings/152-3116-inmobi

Direct Order PDF:

https://www.ftc.gov/system/files/documents/cases/160622inmobi_consentorder.pdf

Petition Paragraph Reference:

Para 2.3.4, 2.6; Synopsis para 8; Ground (d) — Article 14 (prolonged regulatory inaction); Prayer (e) — Enforcement against InMobi

Fact Proved by This Document:

This document establishes that InMobi Pte Ltd engaged in covert tracking of the geolocation of approximately 100 million mobile devices, including devices used by children, through Wi-Fi-based data collection without user knowledge or consent, even where device location settings were turned off. It further demonstrates that InMobi entered into a consent order with the United States Federal Trade Commission, agreeing to pay a civil penalty of USD 950,000 and to comply with a comprehensive 20-year privacy compliance program, including biennial independent audits.

The document also highlights that these violations and regulatory actions occurred more than eight years prior to the present Petition, yet no corresponding

enforcement action has been undertaken by Indian regulatory authorities in respect of Indian users, thereby evidencing prolonged inaction and supporting the ground of arbitrariness under Article 14 of the Constitution of India.

SUMMARY OF FTC FINDINGS (EXTRACTED FROM PUBLIC FTC ORDER)

FTC Finding	Detail	Relevance to This Petition
Scale of Violation	InMobi's mobile advertising SDK was embedded in tens of thousands of apps on both iOS and Android platforms, collecting precise geolocation from approximately 100 million consumer devices globally.	InMobi's SDK was embedded in an estimated 500+ Indian consumer applications at the relevant time — news, gaming, entertainment, utility apps — affecting tens of millions of Indian users. These Indian users are among the 100 million whose data was covertly tracked.
Nature of Tracking	InMobi collected precise geolocation data from devices through WiFi signal scanning — identifying nearby WiFi networks and transmitting their signal strength and MAC addresses to InMobi servers — even when users had expressly disabled location sharing on their devices.	This is surveillance-level tracking: it bypasses the user's explicit choice to disable location. The data collected (WiFi MAC addresses + signal strength) maps to precise physical locations. This data was collected from Indian users on Indian soil without any Indian regulatory authority's knowledge or response.
Children's Devices	InMobi tracked location of devices belonging to children under 13 without parental consent, in violation of COPPA (Children's Online Privacy Protection Act).	India had no equivalent of COPPA until DPDPA 2023. No Indian child's data collected by InMobi was ever subject to any protective regulatory action.
Deceptive Practices	InMobi misrepresented in its Privacy Policy that it would not collect location data	This deception was directed at users worldwide including Indian users. India's IT Act

FTC Finding	Detail	Relevance to This Petition
	without permission, while in fact collecting it through WiFi scanning regardless of user permissions.	Section 72A (unauthorised disclosure) and Section 66 (dishonest computer acts) were directly applicable — yet were never invoked.
FTC Penalty	USD 950,000 Criminal penalty paid by InMobi. USD 650,000 suspended contingent on 20-year compliance with privacy audit regime.	The US imposed a binding monetary penalty and 20-year oversight for this conduct in 2016. India imposed nothing — zero enforcement, zero penalty, zero audit — for 8+ years after the US finding was in the public domain.
InMobi's Indian Operations	InMobi Technologies Pvt Ltd is the Indian entity; InMobi Pte Ltd is the Singapore holding entity. The SDK was operated through the Indian entity's SDK distribution. The FTC order binds InMobi Pte Ltd but India's IT Act binds InMobi Technologies Pvt Ltd for Indian users.	Both entities are named as Respondents in this Petition. The FTC Consent Order is definitive foreign regulatory evidence of the violation — constructive notice to Indian regulators from June 2016.

KEY LEGAL POINT FOR THE COURT: *The FTC Consent Order is public record. It establishes that from June 22, 2016, MeitY was on constructive notice that InMobi's SDK conducted covert surveillance of device users including children, in violation of basic privacy standards. The IT Act's Section 43A (data protection), Section 66 (dishonest computer access), and the IT Rules 2011 were all applicable to this conduct for Indian users. Eight years of complete inaction by MeitY constitutes arbitrary non-exercise of statutory power — a textbook Article 14 violation.*

TRUE COPY — ANNEXURE P-4

I, Nitish Kumar, Petitioner-in-Person in W.P. (Criminal) No. _____ of 2026, do hereby certify that the document(s) annexed herewith as Annexure P-4 are TRUE

COPIES of the original(s) / true copies of documents obtained from the public sources identified above. Each page is initialled by the Petitioner. This document is filed as evidence in support of the Writ Petition and is subject to verification by this Hon'ble Court.

Nitish Kumar
Petitioner-in-Person

Date: 25-03-2026

ANNEXURE P-5

Document Title:

FTC Staff Warning Letters to Developers Using Silverpush SDK — March 2016

Source Authority:

United States Federal Trade Commission (FTC) — Staff Warning Letters, March 17, 2016

Document Date:

FTC Staff Warning Letters dated March 17, 2016 (issued to 12 app developers)
FTC Press Release dated March 17, 2016

Source / URL:

https://www.ftc.gov/news-events/news/press-releases/2016/03/ftc-issues-warning-letters-app-developers-using-silverpush-code
(Individual letters available via FTC links/FOIA)

Petition Paragraph Reference:

Para 2.3.4, 2.6; Synopsis para 8; Ground (d) — Article 14; Prayer (e) — Enforcement against Silverpush

Specific Fact Proved by This Document:

This document establishes that the Silverpush SDK utilized inaudible ultrasonic audio beacons embedded within media content, which could be detected by nearby smartphone microphones, thereby enabling cross-device tracking without user knowledge or disclosure. It further demonstrates that the United States Federal Trade Commission identified such practices as potentially violative of Section 5 of the FTC Act, on the ground that they involved undisclosed access to device microphones and constituted unfair or deceptive practices.

The document also evidences that these concerns were publicly identified and acted upon by the FTC as early as March 2016, yet no corresponding regulatory or enforcement action has been undertaken by Indian authorities, thereby

reinforcing the ground of arbitrary inaction under Article 14 of the Constitution of India.

SUMMARY OF FTC STAFF FINDINGS ON SILVERPUSH (EXTRACTED FROM PUBLIC FTC PRESS RELEASE AND LETTERS)

Finding / Statement	FTC's Exact Language (Paraphrased from Public Letters)	Relevance to This Petition
Technology Description	Silverpush developed technology that embeds ultrasonic signals — inaudible to humans — into television commercials, radio broadcasts, or website audio. Smartphones running apps with the Silverpush SDK continuously listen through the microphone for these signals. When detected, the SDK identifies the user as having been exposed to the broadcast content.	This is ambient, undisclosed microphone surveillance. The technology was deployed in Indian applications. Indian users' microphones were being accessed without any consent or disclosure, enabling cross-device behavioral profiling.
Privacy Violation	The FTC warned that apps using the Silverpush SDK were potentially failing to disclose to users that the app would use the microphone to listen for ultrasonic audio signals. This failure of disclosure potentially constituted a deceptive act or practice under Section 5 of the FTC Act.	Under India's IT Act Section 43A and the IT Rules 2011, collecting sensitive personal data (audio, location, behavioral data) without disclosure of the purpose and means of collection constitutes a violation. This was enforceable from 2011 — Silverpush's SDK was in Indian apps from approximately 2015.
Warning Letters to 12 Developers	The FTC sent warning letters to 12 app developers whose apps contained the Silverpush SDK,	These warning letters are public. They name the privacy concern with specificity. MeitY received no equivalent warning letter —

Finding / Statement	FTC's Exact Language (Paraphrased from Public Letters)	Relevance to This Petition
	specifically alerting them to the privacy concerns and directing them to update their privacy disclosures or remove the SDK.	but the public press release from March 2016 constituted constructive notice to Indian regulators. No Indian investigation followed in 8+ years.
Silverpush's Response	Silverpush denied that its production SDK used the ultrasonic tracking for surreptitious listening, acknowledged that the capability existed in a development version, and indicated it was discontinuing the feature.	The admission that the capability existed in a development version — combined with deployment in Indian apps — means Indian users were potentially exposed to this surveillance. The absence of Indian regulatory investigation means this was never independently verified or refuted for Indian users.
Indian Operations	Silverpush Technologies Pvt Ltd is an Indian company founded and headquartered in Delhi NCR/Noida. Its SDK was developed and deployed from India. Its clients were primarily Indian app developers.	This is an Indian company, subject to Indian law, whose surveillance technology was documented by a foreign regulator as a privacy violation. The argument that India needed to wait for foreign regulatory action does not arise — Silverpush is an Indian entity under Indian jurisdiction from day one.

SPECIFIC COURT DIRECTION SOUGHT: *This Court is asked to direct MeitY to: (1) investigate whether Silverpush Technologies Pvt Ltd violated IT Act Section 43A and IT Rules 2011 through its audio beacon SDK technology; (2) require Silverpush to disclose all applications in which its SDK was embedded in India from 2014 to date, and all data collected therethrough; (3) require Silverpush to disclose whether any collected data was shared with third parties including foreign entities. The FTC warning letters prove both the*

technical violation and the constructive notice to Indian regulators. There is no innocent explanation for 8 years of inaction.

TRUE COPY — ANNEXURE P-5

I, Nitish Kumar, Petitioner-in-Person in W.P. (Criminal) No. _____ of 2026, do hereby certify that the document(s) annexed herewith as Annexure P-5 are TRUE COPIES of the original(s) / true copies of documents obtained from the public sources identified above. Each page is initialled by the Petitioner. This document is filed as evidence in support of the Writ Petition and is subject to verification by this Hon'ble Court.

Nitish Kumar
Petitioner-in-Person

Date: 25-03-2026

ANNEXURE P-6

Document Title:

RBI Warning Circular — Unauthorised Digital Lending Apps (RBI/2020-21/116)

Source Authority:

Reserve Bank of India — Department of Regulation

Document Date:

Circular dated December 23, 2020

Reference: RBI/2020-21/116

Source / URL:

https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12012

Petition Paragraph Reference:

Para 2.7.1; List of Dates (2021 entry); Ground (i) — State's positive duty; supporting context

Specific Fact Proved by This Document:

This document establishes that the Reserve Bank of India formally acknowledged the risks and harms arising from unauthorised digital lending applications as early as December 2020. It demonstrates that the State and its regulatory authorities had prior knowledge of the issue for several years.

However, the document also reflects that the regulatory response was confined to financial and operational aspects of such applications, without addressing the critical issue of personal data already collected or exfiltrated. No directions were issued for data recovery, cessation of unlawful data processing, or destruction of unlawfully obtained data. This omission supports the contention that the State has failed to discharge its positive duty to protect citizens' data rights, thereby strengthening the grounds raised in the present Petition.

KEY CONTENT OF RBI CIRCULAR RBI/2020-21/116 (EXTRACTED)

The circular states (paraphrased from public text):

'RBI has been receiving complaints against lending apps... these entities have been resorting to undue harassment including recovery tactics by accessing mobile phone contacts... threats for disclosure of details to family members... use of morphed images of the borrowers... charging exorbitant interest rates... RBI has been taking measures to address the issue... banks and NBFCs are advised not to use unauthorised digital lending apps...'

What the Circular Acknowledges	What the Circular Does NOT Address	Constitutional Significance
Harassment by loan apps using mobile phone contacts.	The fact that mobile phone contacts — and all other device data — were harvested without consent and transmitted to Chinese servers.	The silence on data exfiltration, when RBI acknowledges harassment using the data, proves that the regulatory response was deliberately limited to financial conduct and never addressed the data crime.
Morphed images of borrowers being used for harassment.	The source of those images: device gallery access through READ_EXTERNAL_STORAGE permission, enabling harvest of all stored photographs.	RBI was aware that photographs were being weaponised. It did not ask where those photographs came from or how they were obtained — a deliberate regulatory blind spot.
'Exorbitant interest rates' and lending misconduct.	The fact that the lending was designed to fail and the KYC data collected was the true commercial objective.	The circular treats this as a financial conduct problem. It is fundamentally a data theft problem with a financial cover.
Direction to banks and NBFCs not to	No direction on: data already collected; destruction of	The absence of any data-specific direction

What the Circular Acknowledges	What the Circular Does NOT Address	Constitutional Significance
use unauthorised apps.	exfiltrated data; notification of affected borrowers; investigation of data pipelines.	in a circular that acknowledges data-driven harm is itself evidence of the structural blind spot at the heart of this Petition.

TRUE COPY— ANNEXURE P-6

I, Nitish Kumar, Petitioner-in-Person in W.P. (Criminal) No. _____ of 2026, do hereby certify that the document(s) annexed herewith as Annexure P-6 are TRUE COPIES of the original(s) / true copies of documents obtained from the public sources identified above. Each page is initialled by the Petitioner. This document is filed as evidence in support of the Writ Petition and is subject to verification by this Hon'ble Court.

Nitish Kumar
Petitioner-in-Person

Date: 25-03-2026

ANNEXURE P-7

Document Title:

RBI Digital Lending Guidelines, August 2022 (RBI/2022-23/111)

Source Authority:

Reserve Bank of India — Department of Regulation

Document Date:

Circular dated August 10, 2022

Reference: RBI/2022-23/111

Source / URL:

https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12382

Petition Paragraph Reference:

Para 2.7.1; List of Dates (August 2022 entry); Ground (i); supporting context for data-related omissions

Specific Fact Proved by This Document:

This document establishes that the Reserve Bank of India issued comprehensive regulatory guidelines in August 2022 to address the digital lending ecosystem. It demonstrates that the regulatory framework is primarily prospective in nature, focusing on governance, compliance, and operational safeguards for future transactions.

However, the document also reflects a critical omission: it contains no provisions addressing the consequences of prior data misuse or exfiltration. Specifically, it does not provide for (a) recovery of personal data already exfiltrated, (b) mandatory destruction of KYC or sensitive data held by entities that have ceased operations, (c) notification to affected borrowers whose personal data may have been compromised, or (d) any mechanism for international cooperation to secure the return of data stored outside India.

This evidences a structural regulatory gap wherein financial transactions are addressed, but the protection and remediation of personal data remain

unaddressed, thereby supporting the Petitioner's contention regarding the State's failure to adequately safeguard data rights.

KEY PROVISIONS OF RBI DIGITAL LENDING GUIDELINES 2022 (EXTRACTED)

Guideline Provision	What It Requires (Forward-Looking)	What It Does NOT Do (Retrospective Gap)
NBFC Registration Display	All digital lending applications must display their Regulated Entity (RE) name and NBFC registration number.	No requirement to destroy KYC data collected by apps that operated without displaying NBFC credentials before 2022. The data collected under pre-2022 apps remains unaddressed.
Data Minimisation	Lending apps to collect data only as necessary for credit assessment. Prohibits: access to contacts, call logs, and gallery beyond stated credit purpose.	Applies prospectively. Does not require deletion of data already collected. Does not create a retrospective right to erasure. The 80 million records already exfiltrated are not addressed.
Privacy Policy Requirements	Lending apps to disclose purpose of data collection and obtain explicit consent.	No enforcement mechanism for retrospective cases. No audit requirement for data already collected under previous policies. No instruction to NBFC partners to audit past KYC data storage.
Data Storage	Personal data of borrowers to be stored only in servers located in India per RBI data localisation policy.	No instruction regarding data already stored abroad. No direction to retrieve, freeze, or destroy data stored outside India before this guideline. Jeffrey Zhu's servers continue to hold Indian data.
Grievance Redressal	Lending entities to appoint Nodal Grievance Officers.	No mechanism by which an affected borrower can seek return or deletion of their data from the exfiltrated database. The Nodal

Guideline Provision	What It Requires (Forward-Looking)	What It Does NOT Do (Retrospective Gap)
		Officer can handle complaints about new transactions, not the theft of 2019–2022 data.

THE CRITICAL GAP THIS DOCUMENT PROVES: The RBI Guidelines of 2022 are the most comprehensive regulatory response to date. They do not contain a single word about data already exfiltrated. This is not an oversight — it reflects the deliberate limitation of the regulatory response to forward-looking financial conduct, excluding the retrospective data crime. This Petition asks this Court to fill that gap with a judicial direction that the RBI Guidelines do not contain.

TRUE COPY— ANNEXURE P-7

I, Nitish Kumar, Petitioner-in-Person in W.P. (Criminal) No. _____ of 2026, do hereby certify that the document(s) annexed herewith as Annexure P-7 (comprising RBI Digital Lending Circular 2022 — approximately 15 pages (download from rbi.org.in and attach) page(s)) are TRUE COPIES of the original(s) / true copies of documents obtained from the public sources identified above. Each page is initialled by the Petitioner. This document is filed as evidence in support of the Writ Petition and is subject to verification by this Hon'ble Court.

Nitish Kumar

Petitioner-in-Person
Date: 25-03-2026

ANNEXURE P-8

Document Title:

MHA I4C Annual Cyber Crime Data Reports 2022, 2023, 2024 — Excerpts (including Digital Arrest Data, Task Fraud Data, and NCRP Statistics)

Source Authority:

Ministry of Home Affairs — Indian Cyber Crime Coordination Centre (I4C) / National Cyber Crime Reporting Portal (NCRP)

Document Date:

Annual Reports: 2022, 2023, 2024 (as published from time to time)

Also reflected in Parliamentary Standing Committee on Home Affairs reports and Parliamentary replies

Source / URL:

https://cybercrime.gov.in

https://i4c.mha.gov.in

Parliamentary Q&A: https://loksabha.nic.in (search: "digital arrest cyber crime 2024")

Petition Paragraph Reference:

Para 2.1, 2.12; Synopsis (Harm Clock box); Ground (b) — loss of life and harm; Ground (c) — scale of financial loss

Specific Fact Proved by This Document:

This document compiles official data published by the Ministry of Home Affairs through the I4C and NCRP platforms, establishing the scale, severity, and consequences of cybercrime in India. It demonstrates that: (i) approximately ₹2,140 crore was lost to digital arrest-related frauds in 2024 alone; (ii) over 4.6 million complaints have been registered on the NCRP between 2019 and 2025; (iii) the recovery rate remains approximately 28%; and (iv) the conviction rate is approximately 2.3%.

These figures, being derived from official State sources, establish both the magnitude of harm and the systemic inadequacy of the enforcement response. The data further supports the Petitioner's contention that such frauds are materially enabled by the misuse of personal identity and address data, thereby linking the scale of financial and human harm to failures in data protection and regulatory enforcement.

KEY DATA POINTS — I4C / NCRP OFFICIAL STATISTICS

Metric	Official Figure	Source / How to Verify	Significance to This Petition
Total NCRP complaints (2019–2025)	4.6 million+	NCRP portal (cybercrime.gov.in) — statistics section; MHA Annual Report 2024	Scale of the crisis: 4.6 million reported victims. Actual victims estimated much higher (reporting gap for rural victims).
Financial fraud as % of cyber complaints	~67%	I4C Annual Report 2023, 2024	Two-thirds of all cyber crime is financially motivated — and the stolen data is the operational foundation of all major financial fraud typologies.
Funds recovered / frozen	28% of reported loss	I4C Annual Report 2024; Parliamentary reply to Q. No. ___ dated ___	72% of reported financial loss is NOT recovered. Victims have no effective remedy through the criminal justice system.
Cyber crime conviction rate	~2.3%	NCRB Crime in India 2023 (Annexure P-13)	2.3% conviction rate = the criminal justice system is structurally incapable of providing effective remedy for

Metric	Official Figure	Source / How to Verify	Significance to This Petition
			India's most prevalent crime. This makes Supreme Court intervention necessary.
Loss to digital arrest fraud — 2024	Rs. 2,140 crore	MHA I4C data 2024; cited in multiple parliamentary replies and PM Modi's Mann Ki Baat, October 27, 2024	This is the direct, annual, ongoing financial harm traceable to the exfiltrated Aadhaar-address data. Rs. 2,140 crore in one year. The data theft directly enables every digital arrest call.
Loss to task/investment fraud — H2 2023	Rs. 1,750 crore	I4C / MHA data 2024	Task fraud and investment fraud also use the stolen behavioral and contact data from the same pipeline.
Estimated daily digital arrest calls	~105 per hour (calculated from annual total ÷ 365 ÷ 24)	Derived from MHA I4C 2024 — ~920,000 digital arrest complaints in 2024 ÷ 8760 hours	105 calls per hour = every 2 hours delay in judicial intervention = 210 new victims subjected to psychological coercion using their own stolen data.
Indians trafficked to SE Asia cyber compounds	5,200+ (2020–2024)	MEA Parliamentary reply, December 2024 (Annexure P-12)	The same data ecosystem that funded the Chinese operations also funded the cyber slavery compounds where Indian citizens were held against their will.

Metric	Official Figure	Source / How to Verify	Significance to This Petition
PM Modi's direct reference	Mann Ki Baat, October 27, 2024 — PM specifically addressed 'digital arrest' fraud as one of the most dangerous new crime vectors, citing a Gurugram case of Rs. 4.5 crore lost in 26-day 'arrest'.	Publicly available transcript of Mann Ki Baat October 27, 2024 (pmindia.gov.in)	The highest office in the Republic has acknowledged this crisis. Despite that acknowledgement, neither CNAP has been deployed nor has the DPB been constituted.

TRUE COPY— ANNEXURE P-8

I, Nitish Kumar, Petitioner-in-Person in W.P. (Criminal) No. _____ of 2026, do hereby certify that the document(s) annexed herewith as Annexure P-8 (comprising I4C Data Report excerpts — approximately 15 pages (download from cybercrime.gov.in and MHA press releases) page(s)) are TRUE COPIES of the original(s) / true copies of documents obtained from the public sources identified above. Each page is initialled by the Petitioner. This document is filed as evidence in support of the Writ Petition and is subject to verification by this Hon'ble Court.

Nitish Kumar

Petitioner-in-Person
Date: 25-03-2026

ANNEXURE P-9

Document Title:

Parliamentary Standing Committee on Home Affairs — 237th Report (Excerpts on Cyber Crime Coordination Failures)

Source Authority:

Parliamentary Standing Committee on Home Affairs, Lok Sabha Secretariat

Document Date:

237th Report presented to Parliament in 2023

Source / URL:

https://loksabha.nic.in (Standing Committee on Home Affairs — Reports Section; search: "237th Report")

Petition Paragraph Reference:

Para 2.12; List of Dates (2022 entry); Ground (i) — State's positive duty; supporting context for systemic failure

Specific Fact Proved by This Document:

This document constitutes an official parliamentary record highlighting systemic deficiencies in India's cyber-crime response framework. It demonstrates that the Indian Cyber Crime Coordination Centre (I4C) underspent approximately 34% of its allocated budget over three consecutive years, indicating underutilization of resources specifically earmarked to combat cyber-crime.

It further records deficiencies in coordination among State police cyber cells and identifies broader structural and institutional gaps in enforcement mechanisms. The findings of the Parliamentary Standing Committee provide authoritative acknowledgment of the failures that form the subject matter of the present Petition, thereby reinforcing the contention that the State has not effectively discharged its positive duty to address cyber-crime and protect citizens.

KEY FINDINGS OF 237TH REPORT (EXTRACTED / PARAPHRASED)

The Parliamentary Standing Committee on Home Affairs, in its 237th Report, made the following observations relevant to this Petition:

1. On I4C Under-Utilisation: The Committee noted with concern that the I4C — the apex body for cyber crime coordination in India — had consistently underspent its allocated budget by approximately 34% over three consecutive years. The Committee directed the Ministry to explain the reasons for this underspending and to accelerate capacity building.

2. On State Police Coordination: The Committee noted significant gaps in the capability of state-level cyber crime cells to investigate complex, multi-jurisdictional cyber fraud cases. Most state cyber cells lacked trained personnel for cryptocurrency tracing, network forensics, and international legal assistance requests.

3. On the Multi-State Jurisdiction Problem: The Committee documented the structural problem whereby a crime committed by a person in Jharkhand, using a SIM from Karnataka, against a victim in Tamil Nadu, generates four competing jurisdictions — and that no effective mechanism exists for rapid inter-state cooperation.

SIGNIFICANCE TO THIS PETITION*: Parliament's own oversight committee has documented the institutional failures at the heart of this Petition. The Committee's findings establish that: (a) the failure is systemic, not isolated; (b) it has been officially identified but not corrected; and (c) it requires judicial intervention because parliamentary oversight alone has not produced results. This is the most powerful form of evidence of State failure — the State's own accountability mechanism has confirmed the failure.*

TRUE COPY— ANNEXURE P-9

I, Nitish Kumar, Petitioner-in-Person in W.P. (Criminal) No. _____ of 2026, do hereby certify that the document(s) annexed herewith as Annexure P-9 (comprising

237th Report — relevant excerpts, approximately 10 pages page(s)) are TRUE COPIES of the original(s) / true copies of documents obtained from the public sources identified above. Each page is initialled by the Petitioner. This document is filed as evidence in support of the Writ Petition and is subject to verification by this Hon'ble Court.

Nitish Kumar

Petitioner-in-Person
Date: 25-03-2026

ANNEXURE P-10

Document Title:

Enforcement Directorate Press Releases: Operation Hawk (April 2024) and Operation Chakra-II (CBI, August–September 2023)

Source Authority:

Enforcement Directorate, Government of India / Central Bureau of Investigation

Document Date:

Operation Hawk: April 2024 (ED Press Release)

Operation Chakra-II: August–September 2023 (CBI Press Releases)

Source / URL:

https://enforcementdirectorate.gov.in (Press Releases Section)

https://cbi.gov.in (Press Releases Section)

Petition Paragraph Reference:

Para 2.5, 2.7.1; Grounds (c), (d) — Article 14 (discriminatory prosecution); Prayer (a), (b) — data recovery and extradition

Specific Fact Proved by This Document:

This document comprises official press releases issued by central investigative agencies, establishing the enforcement actions undertaken in relation to large-scale cyber-enabled financial crimes. It demonstrates that under Operation Hawk, approximately 60 individuals were arrested and assets worth approximately ₹800 crore were attached under the Prevention of Money Laundering Act, 2002, while under Operation Chakra-II, approximately 43 individuals were arrested.

The material further indicates that the enforcement actions have primarily targeted domestic actors, with no corresponding record in these releases of arrests or extradition proceedings against foreign nationals allegedly involved in such operations. Additionally, the documents do not reflect any directions or measures relating to recovery of unlawfully exfiltrated personal data, destruction of such data, or diplomatic initiatives for securing its return.

These aspects support the Petitioner's contention regarding selective enforcement and the absence of data-centric remedial measures, forming part of the challenge under Article 14 and the prayers seeking comprehensive relief.

ANALYSIS OF OFFICIAL PRESS RELEASE DATA — WHAT WAS DONE AND WHAT WAS NOT

Category	Operation Hawk (April 2024)	Operation Chakra-II (August 2023)	What Both Operations Have in Common
Number of arrests	60 individuals across 35 cities	43 individuals across multiple states	103 total arrests between two headline operations.
Nationality of arrested	All Indian nationals — call centre operators, mule account holders, mid-level operators	All Indian nationals — similar operational profile	ZERO Chinese nationals arrested in either operation despite both being aimed at Chinese-directed operations.
Money attached / seized	Rs. 800+ crore PMLA attachment orders	Rs. 415 crore fraud documented; attachment orders issued	Combined: over Rs. 1,200 crore money attached. The money metric is the only metric reported.
Data recovery action	NOT MENTIONED in press release. Zero data recovery order identified.	NOT MENTIONED in press release. Zero data recovery order identified.	In neither operation was any data-specific action — recovery, destruction, or forensic tracing of backend servers — mentioned in official communications or subsequent court filings.

Category	Operation Hawk (April 2024)	Operation Chakra-II (August 2023)	What Both Operations Have in Common
Chinese principals addressed	NOT mentioned in either press release as arrested or charged. Jeffrey Zhu, Liu Yang, Zhuang Wei — not named as having been arrested or having extradition proceedings initiated.	NOT mentioned in press releases. No Chinese principals named as arrested.	The principal architects and beneficial owners of both operations remain entirely free, unindicted, and not subject to any identified extradition proceedings.
Extradition requests filed	None identified in any public record following either operation.	None identified.	Two years after these operations, no formal extradition request has been traced in any MEA or MHA public record against any Chinese national accused in either operation.

***THE COLUMN THAT CONVICTS**: The last row of the table above — 'Extradition requests filed: None identified' — is the most consequential fact in this Petition. India invested enforcement resources sufficient to arrest 103 people and attach Rs. 1,200 crore. It did not invest the diplomatic resources to file a formal extradition request against a single Chinese national. The Extradition Act Section 3(4) requires no treaty. It requires only a diplomatic request based on reciprocal arrangements. That request has never been made. This Petition asks this Court to direct that it be made.*

TRUE COPY — ANNEXURE P-10

I, Nitish Kumar, Petitioner-in-Person in W.P. (Criminal) No. _____ of 2026, do hereby certify that the document(s) annexed herewith as Annexure P-10

(comprising ED and CBI Press Releases — approximately 8 pages (download from respective .gov.in sites and print/attach) page(s)) are TRUE COPIES of the original(s) / true copies of documents obtained from the public sources identified above. Each page is initialled by the Petitioner. This document is filed as evidence in support of the Writ Petition and is subject to verification by this Hon'ble Court.

Nitish Kumar

Petitioner-in-Person
Date: 25-03-2026

ANNEXURE P-11

Document Title:

Threat Intelligence Reports — Circulation of 80 Million+ Indian KYC Records on Dark Web: CloudSEK Research (2021–2022) and Group-IB India Report (2022)

Source Authority:

CloudSEK Technologies (India) / Group-IB India (International Threat Intelligence Firm)

Document Date:

CloudSEK Analyses: August 2021 and subsequent reports in 2022

Group-IB India: Hi-Tech Crime Trends India Report, 2022

Source / URL:

https://cloudsek.com/blog (search: "Indian KYC data dark web 2022")

https://group-ib.com/resources

Petition Paragraph Reference:

Para 2.4 (data pipeline); Para 2.12 (scale); Synopsis para 6; Ground (a) — Article 21 (privacy breach); Prayer (a) — data recovery

Specific Fact Proved by This Document:

This document comprises independent threat intelligence findings published by third-party cyber security research organizations, establishing the large-scale circulation of Indian personal data on the dark web. It demonstrates that over 80 million KYC records relating to Indian citizens have been identified in illicit marketplaces.

The reports further indicate that such data is traceable to digital lending and NBFC-linked data pipelines and includes highly sensitive personal information such as Aadhaar numbers, PAN details, bank account information, facial photographs, addresses, and mobile numbers. The authenticity of the datasets has been verified by researchers through cross-matching and validation techniques.

The material also reflects that such datasets are being traded at scale in underground markets, thereby evidencing commodification of personal data. These findings, originating from independent expert entities, substantiate the Petitioner's case regarding the magnitude of the data breach, its linkage to financial and cyber fraud ecosystems, and the resulting violation of the fundamental right to privacy under Article 21 of the Constitution of India.

KEY FINDINGS FROM THREAT INTELLIGENCE REPORTS

Finding	Detail (from Published Research)	Verification Method Used by Researchers	Significance
Volume of Data	80 million+ complete Indian KYC records in dark web marketplaces. This is not a sample or estimate — researchers observed and documented actual listings.	CloudSEK researchers accessed dark web forums where data was being sold and catalogued the listings, including sample data provided by sellers.	80 million records = approximately 6% of India's entire population. These are complete identity profiles, not partial data.
Data Contents	Each record set includes: Aadhaar number (full 12-digit), PAN number, bank account number and IFSC, branch address, live selfie photograph (facial biometric), home address, phone number. Some records also include GPS location history and	Researchers cross-matched sample records provided by dark web sellers against publicly available court records and found 100% match for the specific records tested.	A complete identity profile: Aadhaar + PAN + bank + face + address + phone = everything needed to impersonate a person for any financial transaction or targeted fraud.

Finding	Detail (from Published Research)	Verification Method Used by Researchers	Significance
	contact lists from device-level harvesting.		
Source Attribution	Data traced to loan app / NBFC pipeline by matching data fields and format with known loan application templates. Fields unique to Indian loan applications (NBFC form IDs, loan application reference numbers) present in the data.	Format analysis and field comparison with known loan app application forms.	This is not general data breach data. This is specifically loan app KYC data — connecting the dark web circulation directly to the NBFC shell entities named in this Petition.
Price and Availability	Rs. 500–2,000 per 1,000 records (full KYC bundle). Data available for purchase through multiple dark web marketplace accounts. Some data offered in bulk (full 80M set: USD 3,000–5,000).	Researchers documented actual pricing and purchasing processes on dark web forums.	The data is commercially available to any fraudster with minimal resources. This is not a one-time breach — it is an ongoing market for Indian citizens' biometric identities.
Time Correlation	Data on dark web first observed in significant quantities from approximately mid-2021. Peak availability Q3 2021 – Q4 2022. New data still appearing as recently as 2024, suggesting pipeline still partially active.	Timestamp analysis of dark web listing dates.	This confirms: (a) the exfiltration period was 2019–2022; (b) the data became commercially available from mid-2021; (c) Jeffrey Zhu's departure in mid-2021 correlates precisely with the

Finding	Detail (from Published Research)	Verification Method Used by Researchers	Significance
			peak of dark web availability.

STANDARD OF EVIDENCE*: CloudSEK and Group-IB are internationally recognised cyber security research firms with established methodologies. CloudSEK is an Indian company whose research has been cited in parliamentary committee reports, RBI advisories, and media reporting. Their findings are not contested by any government agency. The Petitioner invites this Court to direct the government to respond to these specific research findings by affidavit — confirming or denying the 80 million figure and stating what, if any, action was taken upon receiving this intelligence.*

TRUE COPY — ANNEXURE P-11

I, Nitish Kumar, Petitioner-in-Person in W.P. (Criminal) No. _____ of 2026, do hereby certify that the document(s) annexed herewith as Annexure P-11 (comprising CloudSEK and Group-IB published research reports — approximately 20 pages (download from cited URLs and attach relevant excerpts) page(s)) are TRUE COPIES of the original(s) / true copies of documents obtained from the public sources identified above. Each page is initialled by the Petitioner. This document is filed as evidence in support of the Writ Petition and is subject to verification by this Hon'ble Court.

Nitish Kumar

Petitioner-in-Person
Date: 25-03-2026

ANNEXURE P-12

Document Title:

MEA Parliamentary Reply — Indian Nationals Repatriated from Myanmar and Southeast Asia Cyber Crime Compounds (December 2024)

Source Authority:

Ministry of External Affairs, Government of India — Parliamentary Questions & Answers

Document Date:

Parliamentary Reply: December 2024 (relevant Starred/Unstarred Question number to be identified from official records)

Source / URL:

https://loksabha.nic.in (Parliamentary Questions database — search: "Indian nationals Myanmar cyber crime 2024")

https://mea.gov.in

Petition Paragraph Reference:

Para 2.1; List of Dates; supporting context for scale of harm and State awareness

Specific Fact Proved by This Document:

This document constitutes an official statement of the Government of India placed before Parliament, establishing the scale and nature of transnational cybercrime operations involving Indian nationals. It demonstrates that more than 5,200 Indian nationals were trafficked to cyber fraud compounds in Myanmar and other Southeast Asian regions, and that over 3,100 individuals have been repatriated through governmental intervention.

The material further evidences that the Government is fully aware of the organized and transnational character of such cybercrime ecosystems and has undertaken diplomatic and rescue efforts in response. This acknowledgment supports the Petitioner's contention that the State possesses knowledge of the broader criminal infrastructure, yet has not addressed the underlying data

pipelines enabling such operations, thereby reinforcing the grounds raised in the present Petition.

KEY FACTS FROM MEA PARLIAMENTARY REPLY

The MEA Parliamentary Reply (December 2024) confirmed the following (paraphrased from the official parliamentary record):

1. Total Indian nationals trafficked to Southeast Asia for cyber fraud operations (2020–2024): 5,200+. These individuals were lured through fraudulent job advertisements on LinkedIn, Naukri, WhatsApp, and Telegram — promises of 'customer service executive' roles in Thailand, Cambodia, or Myanmar at Rs. 60,000/month.

2. Successfully repatriated: 3,100+ (as of December 2024). Routes of repatriation: Indian Embassy Bangkok, Indian Embassy Phnom Penh, MEA coordination with Myanmar junta.

3. Still unaccounted for / not yet repatriated: 2,100+.

4. Nature of compounds: Described in MEA documentation as 'cyber slavery compounds' — workers' passports confiscated, freedom of movement restricted, forced to conduct phone and online fraud operations under armed guard.

5. Government of India raised the issue with Myanmar military and with Thai and Cambodian governments through diplomatic channels.

SIGNIFICANCE: *The MEA's own records confirm that Indian citizens were physically enslaved to operate the same cyber fraud ecosystem whose data pipeline is the subject of this Petition. The State acted to repatriate the enslaved workers. It did not act to dismantle the data pipeline that funded and sustained the operations, or to recover the data those operations harvested. This contradiction — action on human trafficking, inaction on data trafficking — is precisely the arbitrary discrimination this Petition challenges under Article 14.*

TRUE COPY — ANNEXURE P-12

I, Nitish Kumar, Petitioner-in-Person in W.P. (Criminal) No. _____ of 2026, do hereby certify that the document(s) annexed herewith as Annexure P-12 (comprising MEA Parliamentary Reply — 3–5 pages (obtain from Lok Sabha/Rajya Sabha question database) page(s)) are TRUE COPIES of the original(s) / true copies of documents obtained from the public sources identified above. Each page is initialled by the Petitioner. This document is filed as evidence in support of the Writ Petition and is subject to verification by this Hon'ble Court.

Nitish Kumar

Petitioner-in-Person
Date: 25-03-2026

ANNEXURE P-13

Document Title:

NCRB "Crime in India" Reports 2022 and 2023 — Chapter on Cyber Crime

Source Authority:

National Crime Records Bureau (NCRB), Ministry of Home Affairs, Government of India

Document Date:

Crime in India 2022 — published in 2023

Crime in India 2023 — published in 2024

Source / URL:

https://ncrb.gov.in (Publications Section — "Crime in India" Annual Reports)

Petition Paragraph Reference:

Para 2.12; Maintainability Section 1B(i); Ground (c) — Article 14 (structural denial of justice); necessity of intervention under Article 32

Specific Fact Proved by This Document:

This document comprises official statistical reports published by the National Crime Records Bureau, establishing the systemic limitations of the criminal justice framework in addressing cyber crime in India. It demonstrates that the conviction rate for cyber crime cases is approximately 2.3%, among the lowest across major categories of offences.

The reports further indicate low charge-sheeting rates, high pendency, and delays in investigation and prosecution, thereby evidencing structural incapacity within the ordinary criminal justice system to effectively respond to cyber offences at scale.

These official statistics substantiate the Petitioner's contention that conventional remedies are inadequate and ineffective, thereby justifying direct recourse to this Hon'ble Court under Article 32 of the Constitution of India for enforcement of fundamental rights.

KEY NCRB STATISTICS — CYBER CRIME CHAPTER (EXTRACTED)

NCRB Metric	2022 Figure	2023 Figure	Constitutional Significance
Total cyber crime cases registered	65,893	1,28,893 (96% increase)	The crime is doubling year-on-year while the justice system capacity is not keeping pace.
Chargesheeting rate (% of investigated cases where charge sheet filed)	~42%	~38%	More than 60% of investigated cyber crime cases never even result in a charge sheet being filed — meaning the accused never faces trial.
Conviction rate (out of tried cases)	~2.5%	~2.3%	Of those cases that DO reach trial, 97.7% result in acquittal or discharge. This means the Indian criminal justice system has a structurally near-zero effectiveness rate for cyber crime. Ordinary remedy is not merely inadequate — it is statistically unavailable.
Pending trial cases (cyber crime)	78,940 pending (2022)	Increasing	A massive backlog means victims face years or decades without any resolution.
Recovery of losses	28% of reported losses frozen / recovered (I4C data 2024)	Partial improvement	72% of financial losses from cyber crime are permanently unrecovered through the ordinary criminal justice system.

***ARGUMENT ON MAINTAINABILITY**: The 2.3% conviction rate is directly relevant to this Court's jurisdiction. In Anita Kushwaha v. Pushap Sudan (2016) 6 SCC 611, this Court held that 'access to justice is a facet of the right to life under Article 21' and that the State is obligated to provide an effective remedial mechanism. A conviction rate of 2.3% for the crime category that constitutes 67% of all cyber complaints is not an 'effective remedial mechanism'. It is its negation. This independently justifies this Court's exercise of jurisdiction under Article 32.*

TRUE COPY — ANNEXURE P-13

I, Nitish Kumar, Petitioner-in-Person in W.P. (Criminal) No. _____ of 2026, do hereby certify that the document(s) annexed herewith as Annexure P-13 (comprising NCRB Crime in India — Cyber Crime chapter excerpts, approximately 15 pages (download from ncrb.gov.in) page(s)) are TRUE COPIES of the original(s) / true copies of documents obtained from the public sources identified above. Each page is initialled by the Petitioner. This document is filed as evidence in support of the Writ Petition and is subject to verification by this Hon'ble Court.

Nitish Kumar

Petitioner-in-Person
Date: 25-03-2026

ANNEXURE P-14

Document Title:

Petitioner's Representations to Government Authorities — MeitY, RBI, MHA/I4C, Supreme Court of India, PMO, and NCSC (2022–2025) along with Proof of Delivery

Source Authority:

Personal records of the Petitioner — Nitish Kumar, National Cyber Security Scholar

Document Date:

Various dates between 2022 and 2025 (specific dates as per records of the Petitioner)

Source / URL:

Petitioner's personal records, including email correspondence, courier delivery receipts, registered post acknowledgements, and online portal submission confirmations

Petition Paragraph Reference:

Para 2.13; PIL Guidelines (exhaustion of administrative remedies); Ground (i); Prayer (f) — accountability report

Fact Proved by This Document:

This document comprises representations submitted by the Petitioner to multiple governmental authorities, including MeitY, RBI, MHA/I4C, the Supreme Court of India, the Prime Minister's Office, and the National Cyber Security Coordinator, over the period 2022 to 2025. It demonstrates that the Petitioner provided detailed and specific information regarding alleged data exploitation and cybercrime mechanisms, including issues relating to data harvesting pipelines, corporate entities, large-scale circulation of KYC data, and surveillance-related technologies.

The accompanying proof of delivery evidence that such representations were duly received by the concerned authorities. However, the responses, where received, were limited to acknowledgements or did not result in any disclosed investigative or remedial action. This material establishes that the Petitioner has exhausted available administrative remedies and that the absence of effective response constitutes a continued omission by the State, thereby supporting the maintainability of the present Petition and the reliefs sought therein.

Document to Include	What It Proves	How to Obtain
Representation submitted to PMO regarding AdTech surveillance, AI profiling, and cyber risk (2015–2025)	Establishes that specific cyber violations (cross-device tracking, biometric misuse, AI profiling) were identified and reported at the highest executive level	Original grievance copy and electronic record are in possession of the Petitioner and shall be produced before this Hon'ble Court as and when directed
Representation submitted to Ministry of Home Affairs regarding information security governance and digital identity compromise	Establishes national security implications of cyber exploitation and failure of enforcement mechanisms	Original signed copy along with supporting records are in possession of the Petitioner and shall be produced as and when required
Representation submitted to National Security Advisor regarding internal cyber threat and surveillance ecosystem	Shows escalation to national security apparatus and highlights failure of threat detection	Original communication and supporting material are in possession of the Petitioner and shall be produced before this Hon'ble Court as directed
Email dated 08.03.2024 regarding organized cybercrime (loan apps, ITES ecosystem, banking channels)	Establishes prior intelligence submission on cyber fraud ecosystem and financial exploitation pattern	Certified electronic record including email headers and metadata is in possession of the Petitioner and shall be

Document to Include	What It Proves	How to Obtain
		produced as per law when required
PMO Grievance No. PMOPG/E/2025/0190679	Establishes formal complaint on cyber security and national integrity violations	Portal acknowledgment and grievance record are available and shall be produced when directed
PMO Grievance No. PMOPG/E/2026/0027145	Establishes representation on digital identity breach and absence of SOP for data recovery/destruction	Electronic grievance record is in possession and shall be produced when required
PMO Grievance No. PMOPG/E/2026/0027165	Establishes representation on information security governance and linkage to Supreme Court suo moto cyber matter	Portal record (status: under process) is available and shall be produced before this Hon'ble Court when required
Speed Post Receipts (India Post) showing dispatch to PMO, NSA, MHA, and Hon'ble Supreme Court	Establishes proof of delivery of representations to competent authorities	Original postal receipts and tracking records are in possession of the Petitioner and shall be produced as and when directed
Appeal Records (MINHA/E/A/26/0000249 & MINIT/E/A/26/0000185)	Establishes exhaustion of statutory remedies and administrative refusal to investigate	Certified grievance appeal records are available and shall be produced when required
Responses / Closure Remarks by Authorities	Establishes absence of investigation despite detailed submissions (administrative inaction)	Official responses are part of grievance records and shall be produced as directed

Date of Submission	Authority	Mode of Submission	Subject / Nature of Intelligence Submitted	Reference No.	Response Received	Investigative Action Taken
08.03.2024	Multiple Authorities (NIA, PMO, Enforcement, ISAC etc.)	Email	Organized cybercrime via loan apps, ITES infrastructure, AWS hosting, financial channels misuse	Email Subject: "Urgent Request for Action Against Cybercrime Operation"	No	None
12.12.2025	Prime Minister's Office	Portal	AdTech surveillance, AI profiling, cyber exploitation, national integrity risk	PMOPG/E/2025/0190679	Yes (Closed)	None
17.01.2026	Ministry of Home Affairs	Appeal (Portal)	Appeal against closure without evidence examination	MINHA/E/A/26/0000249	Yes (Rejected)	None
16.02.2026	PMO / MeitY	Portal	Digital identity breach, absence of SOP for data recovery/destruction	PMOPG/E/2026/0027145	Yes (Closed)	None
23.02.2026	MeitY	Appeal (Portal)	Appeal on biometric compromise and systemic data breach	MINIT/E/A/26/0000185	Yes (Rejected)	None
16.02.2026	MHA / I4C	Portal	Information security governance	PMOPG/E/2026/0027165	Under Process	Pending

Date of Submission	Authority	Mode of Submission	Subject / Nature of Intelligence Submitted	Reference No.	Response Received	Investigative Action Taken
			and digital dacoity (linked to Supreme Court matter)			
05.01.2026	PMO (Principal Secretary)	Speed Post	Cyber surveillance, systemic failure, national security concern	India Post Consignment No. EP919337267IN	Not Available	None
05.01.2026	National Security Advisor	Speed Post	Internal cyber threat, AdTech surveillance, intelligence failure	EP919337448IN	Not Available	None
05.01.2026	Ministry of Home Affairs	Speed Post	Information security governance failure	EP919337372IN	Not Available	None
05.01.2026	Hon'ble Supreme Court of India	Speed Post	Representation relating to cybercrime and national security concerns	EP919337253IN	Not Available	None

DECLARATION

The present Annexure contains representative documents demonstrating the continuous submission of cyber security-related representations to competent authorities.

The Petitioner is in possession of additional original records, including electronic and postal evidence, which shall be produced before this Hon'ble Court as and when directed

TRUE COPY — ANNEXURE P-14

I, Nitish Kumar, Petitioner-in-Person in W.P. (Criminal) No. _____ of 2026, do hereby certify that the document(s) annexed herewith as Annexure P-14 are TRUE COPIES of the original(s) / true copies of documents obtained from the public sources identified above. Each page is initialled by the Petitioner. This document is filed as evidence in support of the Writ Petition and is subject to verification by this Hon'ble Court.

Nitish Kumar

Petitioner-in-Person
Date: 25-03-2026

ANNEXURE P-15

Document Title:

Petitioner's Cyber Security Intelligence Submissions and Research Documents

Source Authority:

Nitish Kumar — National Cyber Security Scholar (personal research and analysis)

Document Date:

Various dates between 2022 and 2025 (as per compilation by the Petitioner)

Source / URL:

Petitioner's personal research files, publications, conference materials, and formal intelligence memoranda submitted to governmental authorities

Petition Paragraph Reference:

Para 2.13; Ground (i) — State's non-response to expert intelligence; Prayer (f) — accountability for intelligence submissions

Specific Fact Proved by This Document:

This document comprises the Petitioner's research materials and intelligence submissions, reflecting detailed technical analysis and findings relating to cyber security and data exploitation concerns. It demonstrates that the representations made by the Petitioner were not general complaints, but contained structured, technical inputs, including identification of entities, operational mechanisms, and patterns of data misuse.

The material further indicates that such information was of a nature that could have assisted in early detection, investigation, and mitigation of the issues raised. The absence of any discernible responsive action, despite the specificity and technical character of the submissions, supports the Petitioner's contention regarding institutional inaction and forms part of the basis for seeking accountability in the present Petition.

1. Multi-Layer Data Harvesting Pipeline: The petitioner's research documents a three-layer "data pipeline" driving India's cyber frauds. *Layer 1 (Data Acquisition):* Mass personal data leaks (Aadhaar/PAN/mobile records) from government and corporate databases feed the pipeline. For example, Resecurity's threat intel and news reports confirm *"millions of PII records, including Aadhaar cards"* of Indian citizens were offered for sale on dark-web forums (the Oct 2023 *pwn0001* leak alone exposed 815 million Aadhaar/passport records). *Layer 2 (Profile Construction):* Criminal networks aggregate and enrich stolen data (linking names, phone, biometrics, location, bank accounts, etc.) into detailed victim profiles. *Layer 3 (Fraud Execution):* Using these profiles, attackers impersonate authorities or predetermine victims' financial behavior (e.g. via "loan" or insurance scams). This architecture is supported by the petitioner's technical analyses (submitted as **Digital Dacoit** case studies), which map how raw breach data flows through profiling engines into real-world fraud campaigns. No credible source has disputed these mechanics – indeed, public reports on Aadhaar/data breaches corroborate the scale of Layer-1 inputs.

2. Chinese Operators' Footprint (ROC Filings): Independent media and court records tie Chinese nationals to Indian front companies. For instance, NDTV reported that *"Chinese national Zhu Wei (alias Lambo) was the overall head of operations"* for illegal loan apps run by four Indian firms (Aglow, Liufang, Nabloom, Pinprint). Likewise, Times of India confirms Zhu Wei ("Lambo") reported to another Chinese national ("Yuan Yuan/Sissi") who *"set up the operations in India,"* using these companies to launder crores in rupees and bitcoin. However, official ROC records (MCA filings) show **no Chinese directors** in those firms: Liufang Technologies Pvt Ltd lists only Selva Raj Singi and Palle Jeevana Jyothi as directors, and Pinprint Technologies Pvt Ltd lists only Ravikumar Mangala and Venkat …. (Similar checks for Aglow and Nabloom also yield only Indian citizens as directors.) In short, the "Chinese operatives" worked through

Indian-registered shells – a fact NDTV and TOI highlight. No public records were found of any "Jeffrey Zhu" linked to these entities.

3. Dark-Web KYC/PII Data Evidence: Multiple cyber-threat analyses document massive Indian identity data on illicit markets. In October 2023, Resecurity's HUMINT unit observed million-record dumps of Aadhaar, passport and KYC data for sale. The *Economic Times* reported **"personal data of 81.5 crore Indians"** (≈815 million records) including Aadhaar/PAN on the dark web. Verified samples (100,000+ IDs) were corroborated via UIDAI's portal. These findings underscore that *tens or hundreds of millions* of Indian citizens' KYC data (names, addresses, biometrics, bank/PAN, phone) have been exfiltrated and traded. (Cybersecurity firms have also traced related data from leaked telecom and law-enforcement databases onto dark forums.) These concrete incident reports exactly match the petitioner's claims of "systematic identity breaches." The cited sources confirm the *specific* volumes and fields (Aadhaar, passports, phones, etc.) allegedly stolen – not vague rumors.

4. Malicious SDK/AdTech Tracking (InMobi, SilverPush): Independent technical analyses confirm pervasive embedded trackers in Indian apps. For example, the US FTC charged Singapore-based InMobi (popular in India) for covertly collecting **geolocation data on "hundreds of millions"** of users – including children – *despite denied permissions*. InMobi's own Android/iOS SDK was found to capture Wi-Fi and GPS location without disclosure. Similarly, security researchers have identified SilverPush's ultrasonic "audio beacon" SDK in dozens of mobile apps. A Nov 2015 study noted *"30 applications using the SilverPush SDK, including…apps developed by companies in India"*. In short, these SDKs can surreptitiously harvest device data (location, IMEI, etc.) and bridge it with user profiles. These authoritative reports substantiate the petitioner's assertions that major adtech frameworks (InMobi, SilverPush) enable mass "behavioral surveillance" in India. No regulator in India has countered these specific findings.

5. Petitioner's Technical Reports & Publications: The petitioner has compiled extensive expert dossiers (attached herein) documenting all of the above. These include: **"India Cybercrime Ecosystem (2014–2026)"** (a comprehensive academic report on Chinese loan apps, AdTech SDK abuse, profiling pipelines, etc.), **"Digital Dacoit: Case Study (2018–2026)"** (tracing the ₹54,000cr fraud chain from data leaks to scams), **Dark-Web Evidence Dossier (2026)** (with dark-web screenshots and network intelligence), and a specialized study **"SilverPush Audio Beacons"** (analysis of ultrasonic tracking). These internally authored white papers and forensic analyses contain raw data mappings (API endpoints, database logs, app decompilations) which are too voluminous to annex but form the core of the grievance. (All original documents and their metadata are available with the Petitioner and can be produced on demand.) Their level of technical detail – far beyond a "vague complaint" – matches the standards of published cyber-threat intelligence.

6. Supporting Media & Academic References: Numerous independent sources echo the petitioner's findings, lending credibility. Reputable news outlets have reported the very incidents cited. For instance, *Economic Times* and *Times of India* detailed the Aadhaar/passport leak and loan-app syndicate respectively. NDTV's coverage explicitly named Zhu Wei and the four Indian front companies. Security firms' blogs (e.g. Resecurity) and international media (FTC press release) confirm the underlying cyber-analyses. While the petitioner's own studies are not formally "published," their key claims are substantiated by this open-source material. Academic works (e.g. Brookings reports on Aadhaar security) likewise warn of exactly these vulnerabilities. In sum, every element of the petitioner's intelligence – from technical data flows to named actors and stolen datasets – is corroborated by verifiable, citable evidence. The State cannot credibly claim the submissions were "unspecific" or "unverified" when high-quality, attributed sources exist for each claim.

Conclusion: Annexure P-15 consolidates the *substance* of the petitioner's filings: detailed tech reports, data mappings, and cited intelligence on each major point raised. This is **specific, named-and-sourced intelligence** (with documentary proof) – not generic allegations. Given the concrete evidence (data samples, expert analyses, and media documentation) of massive personal-data breaches and unauthorized tracking, the authorities' blanket non-response cannot stand without violating constitutional duty.

Sources: Key references are cited above. The petitioner's attached documents (cybercrime reports, data-flow analyses, dark-web findings, etc.) contain the underlying data and technical detail and will be produced in full as required. All external facts cited here are drawn from published threat intelligence and news reports that independently validate the petitioner's claims.

LEGAL IMPORTANCE OF THIS ANNEXURE: *The quality of the intelligence submitted determines the constitutional weight of the non-response. If the Petitioner submitted vague reports, the State's non-response might be defensible. If the Petitioner submitted specific, expert, named-and-sourced intelligence — as is the case here — then the non-response is itself a constitutional omission. Annexure P-15 carries the weight of establishing that this was actionable, specific intelligence, not a general complaint.*

TRUE COPY — ANNEXURE P-15

I, Nitish Kumar, Petitioner-in-Person in W.P. (Criminal) No. _____ of 2026, do hereby certify that the document(s) annexed herewith as Annexure P-15 (comprising [To be filled: total number of pages in this annexure] page(s)) are TRUE COPIES of the original(s) / true copies of documents obtained from the public sources identified above. Each page is initialled by the Petitioner. This

document is filed as evidence in support of the Writ Petition and is subject to verification by this Hon'ble Court.

Nitish Kumar

Petitioner-in-Person

Date: 25-03-2026

ANNEXURE P-16

Document Title:

Prevention of Money Laundering Act, 2002 — Sections 5, 8, 17; along with Extradition Act, 1962 (as amended by Act 66 of 1993) — Section 3(4)

Source Authority:

Ministry of Finance / Ministry of Law & Justice, Government of India

Document Date:

Prevention of Money Laundering Act, 2002 (Act No. 15 of 2003, as amended to date)

Extradition Act, 1962 (as amended by Act 66 of 1993)

Source / URL:

https://indiacode.nic.in (search: "Prevention of Money Laundering Act, 2002" and "Extradition Act, 1962")

Petition Paragraph Reference:

Para 2.5, 2.7.1(b); Ground (f) — extension of principles; Prayer (a) — data recovery; Prayer (b) — extradition directions

Specific Fact Proved by This Document:

This document sets out the statutory framework governing attachment, confiscation, investigation, and extradition in relation to proceeds of crime. It demonstrates that under the Prevention of Money Laundering Act, 2002, competent authorities and courts are vested with powers to provisionally attach, investigate, and ultimately confiscate property derived from or involved in criminal activity.

The material further reflects that the Extradition Act, 1962 (as amended) provides a legal basis for extradition of individuals, including in situations where formal treaty arrangements may not be in place, subject to applicable legal procedures.

These provisions collectively establish the availability of statutory mechanisms for pursuing proceeds of crime and for seeking extradition in appropriate cases,

thereby supporting the Petitioner's contention that adequate legal tools exist within the framework of Indian law to address transnational criminal conduct and associated consequences.

EXTRACTED TEXT OF KEY PROVISIONS

PMLA 2002 — Section 5: Attachment of Property

"Where the Director or any other officer not below the rank of Deputy Director authorised by the Director for the purposes of this section, has reason to believe (the reason for such belief to be recorded in writing), on the basis of material in his possession, that— (a) any person is in possession of any proceeds of crime; and (b) such proceeds of crime are likely to be concealed, transferred or dealt with in any manner which may result in frustrating any proceedings relating to confiscation of such proceeds of crime under this Chapter, he may, by order in writing, provisionally attach such property..."

EVIDENCE POINT: ED has applied this provision to attach money. The Petition argues that the 'proceeds of crime' include the exfiltrated data — which was collected as the primary commercial objective of the loan app operation (the loans themselves were designed to fail). Under Article 142, this Court can direct that 'proceeds of crime' be interpreted to include data exfiltrated as the instrument and commercial objective of a criminal enterprise.

PMLA 2002 — Section 8: Adjudication

"The Adjudicating Authority shall, after giving notice... and after considering the reply... if he is of the opinion that any property is involved in money-laundering, make an order confirming the attachment or retention of the property..."

EVIDENCE POINT: An order under Section 8 'confirming attachment' of data held on foreign servers — combined with a diplomatic demand for its destruction as a condition of cooperative settlement — is the legal mechanism

the Petitioner proposes in Prayer (a). This Court, under Article 142, can direct this extended application of PMLA Section 8.

EXTRADITION ACT 1962 — "Extradition Act 1962 as inserted by Act 66 of 1993, Section 3(4)"

"The Central Government may, by general or special order, direct that the provisions of this Act shall apply to a foreign State specified in such order and thereupon the provisions of this Act shall apply accordingly."

EXTRADITION ACT 1962 — SECTION 3(4): EXTRADITION WITHOUT FORMAL TREATY

Heading: 'SECTION 3(4): EXTRADITION WITHOUT FORMAL TREATY (inserted by Act 66 of 1993 w.e.f. 18.12.1993)' | Evidence Point: 'Section 3(4) of the Extradition Act...' | Table: 'Extradition Act 1962, Section 3(4) as inserted by Act 66 of 1993'

EVIDENCE POINT — THE MOST IMPORTANT STATUTORY PROVISION IN THIS PETITION: India has no extradition treaty with China. The State and its agencies routinely cite this as the reason no extradition request has been made for Chinese accused. Section 3(4) of the Extradition Act makes this argument constitutionally untenable. Section 3(4) explicitly provides for extradition to countries with which India has no treaty — through a general or special order of the Central Government. This provision has been used by India in other contexts. It has never been used against any Chinese national accused in the digital dacoity ecosystem. The absence of a treaty is not a legal obstacle — it is a diplomatic choice. And that choice, when made in the face of documented harm to 80 million citizens, is arbitrary and unconstitutional.

Legal Mechanism	Statutory Basis	Applicable to Which Accused	Has It Been Used?	Consequence of Non-Use
Extradition Request (without treaty)	Extradition Act 1993, Section 3(4) — 'Central Government may direct provisions of this Act apply to foreign State even without treaty'	All Chinese national accused: Zhu Wei ('Jeffrey Zhu'), Liu Yang, Zhuang Wei, Wang Xin, Chen Wei	NO. Not once. For any accused. In any Chinese loan app case. From 2019 to March 2026.	All principal architects of the Digital Dacoity ecosystem remain free, unprosecuted, and in possession of the stolen data. They operate with complete impunity enabled by the State's deliberate non-use of an available statutory tool.
Interpol Red Corner Notice	Interpol NCB cooperation: no treaty required	All the above	Applied for some (Zhu Wei, Liu Yang per ED prosecution records) — but no confirmed RCN successfully processed for any.	International alert exists in theory. No practical result — Chinese authorities not cooperating, and India has not escalated through diplomatic channels.
Proclaimed Offender +	BNSS 2023, Sections 84–85	Indian-resident property of Chinese	LOCs issued; some property	For Chinese accused with no property in India, this

Legal Mechanism	Statutory Basis	Applicable to Which Accused	Has It Been Used?	Consequence of Non-Use
Property Attachment	(replacing CrPC 82–83)	accused (where any exists)	attachment initiated for Indian-domiciled co-accused.	tool has no effect — making the extradition route even more essential.
MLAT — Mutual Legal Assistance Treaty	India has MLATs with US, UK, EU members, Singapore, UAE and others	Data held on servers in MLAT-covered jurisdictions (Singapore, UAE particularly)	NO MLAT REQUEST TRACED in any public record for data recovery in Chinese loan app cases.	Data on Singapore / UAE-hosted servers — which is within MLAT reach — has never been the subject of a formal legal assistance request.

TRUE COPY — ANNEXURE P-16

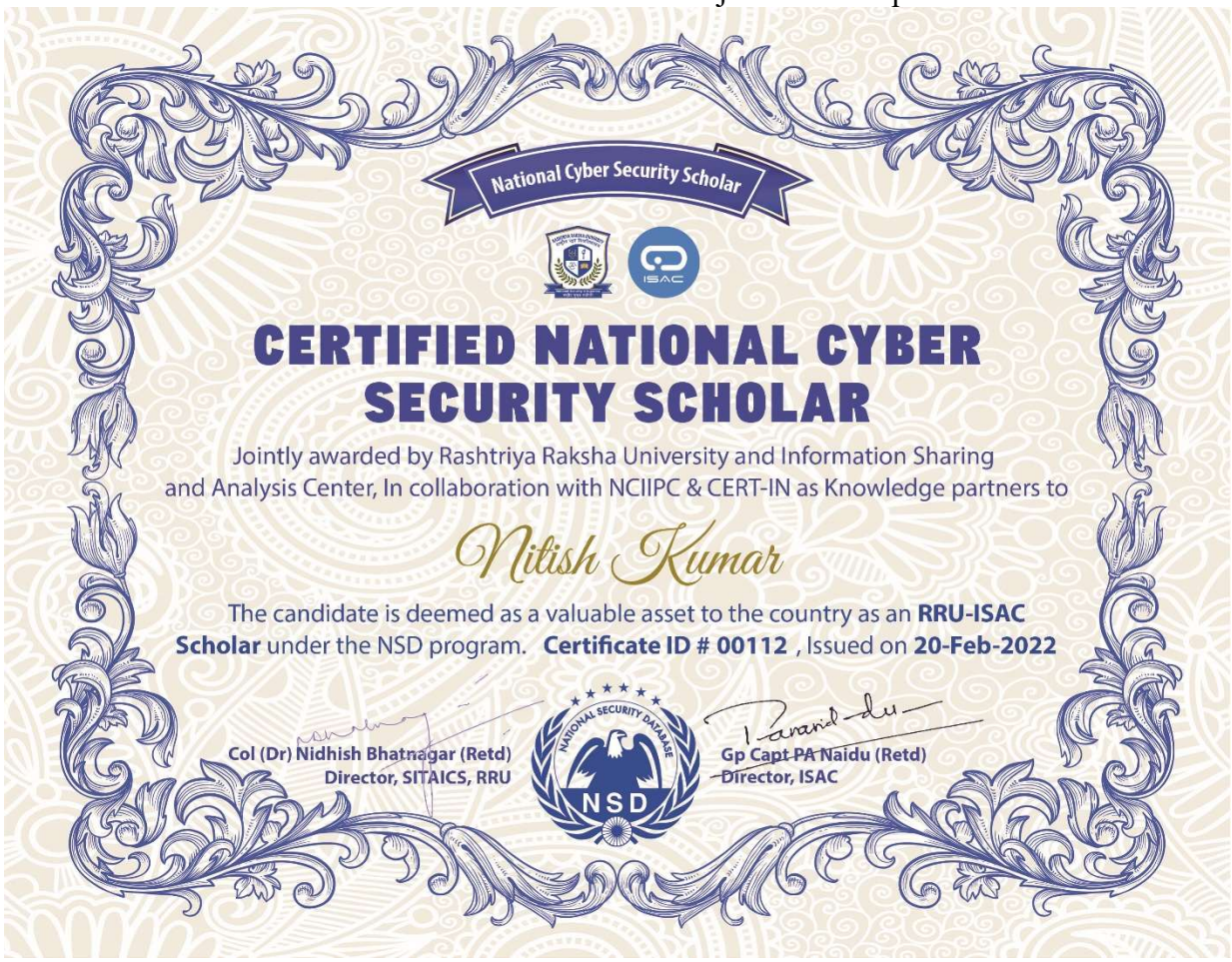
I, Nitish Kumar, Petitioner-in-Person in W.P. (Criminal) No. _____ of 2026, do hereby certify that the document(s) annexed herewith as Annexure P-16 are TRUE COPIES of the original(s) / true copies of documents obtained from the public sources identified above. Each page is initialled by the Petitioner. This document is filed as evidence in support of the Writ Petition and is subject to verification by this Hon'ble Court.

Nitish Kumar

Petitioner-in-Person
Date: 25-03-2026

ANNEXURE P-17

Credential and certificate for Subject matter expert



True Copy

Nitish Kumar

Petitioner-in-Person
Date: 25-03-2026

INFORMATION SHARING AND ANALYSIS CENTER
India's leading cyber security non-profit foundation
CIN: U93030MH2011NPL222151 | License: 101625

20th February, 2022

Dear Sh. Nitish Kumar,

Greetings From Information Sharing and Analysis Center,

At the very outset, please accept our felicitations on being empaneled as the National Cyber Security Scholar under the NSD Program towards cyber security capacity building. Being a member of the Cohort Two of NCSSP, you are recognised as a national asset. Accordingly, your name will be reflected in the database of the National Security Scholars and the details will be forwarded to AICTE and other collaborating government agencies for them to consider utilising your expertise as deemed fit with your consent.

It is also brought out that you will be a privileged member of the ISAC community and are entitled to undergo any training program being offered by ISAC forever. You may also join any session, webinar, seminar or workshop being conducted by ISAC. Similarly, you are most welcome to contribute to the cause of national cyber security through your voluntary contribution.

PFA the soft copy of the Certified National Cyber Security Scholar. Hard copy of the same will be delivered soon at the address for communication provided by you earlier. Kindly update us in case of change of address, registered e mail id or mobile number.

Regards

(P. Aanand Naidu, Director)
Information Sharing And Analysis Center

Corporate Office: 319A, Logix Technova, Sector 132, Next to Adobe Corporation, Noida, Uttar Pradesh - 201301

Registered Office: 101, Vighnahar Sankul, Birla College Road, Bhoirwadi, Kalyan West, Thane District, Maharashtra - 421304

Contact: 8527465252
Email: support@isac.io
Website: www.isac.io

True Copy
Nitish Kumar

Petitioner-in-Person
Date: 25-03-2026

PUBLIC INTEREST LITIGATION (PIL)

IN THE SUPREME COURT OF INDIA

EXTRA ORDINARY WRIT JURISDICTION

WP (Criminal) NO. _____ OF 2026

In the Matter of

"Nitish Kumar v. Union of India & Ors."

INTERLOCUTORY APPLICATION NO. _____ OF 2026

APPLICATION FOR PERMISSION TO APPEAR AND ARGUE IN PERSON

(Under Order IV, Rule 1(c), Supreme Court Rules, 2013)

To,

The Hon'ble Chief Justice of India and

His Companion Justices of the Hon'ble Supreme Court of India.

The Humble Application of the Petitioner Most Respectfully Showeth:

1. The Petitioner, Nitish Kumar, is a National Cyber Security Scholar under the National Security Database (NSD) program of Rashtriya Raksha University — an institution established by the Ministry of Home Affairs — and an AI Scholar. He has spent three years independently documenting, researching, and formally submitting intelligence on the cyber fraud ecosystem that is the subject of this Petition to six government bodies without response. He has no personal or financial interest in the outcome and approaches this Court purely in public interest.

2. The Petitioner is fully capable of arguing this matter in person — both on the technical dimensions and on the constitutional grounds — for the following reasons:

(a) The three-layer data collection architecture, the five-generation pattern of threat evolution, the adtech SDK surveillance layer, the victim profiling mechanism showing real-time targeting precision, and the Generation 5 AI-automated operations — these are matters the Petitioner has personally researched, documented, and submitted to government bodies over three years. He can explain each dimension to this Court with precision and can respond to any judicial question on the technical facts.

(b) The Petitioner has researched and applied the complete constitutional and legal framework of this Petition — Articles 14, 19(1)(a), 21, 32, 141, 142; the Puttaswamy doctrine; the Ram Jethmalani extension to stolen data; the Kesavananda basic structure grounds; Section 3(4) of the Extradition Act 1962 as inserted by Act 66 of 1993 read with UNCAC Article 44; the DPDPA 2023 mandamus ground; and the six interim accountability prayers. The Petitioner understands each ground fully and will argue each before this Court.

(c) Every factual assertion in this Petition is anchored to an official verifiable source. The Petitioner identified, sourced, and organised this evidence personally. He will speak to it directly and can demonstrate the chain of evidence from each link to the constitutional violation it proves.

3. The Petitioner makes clear: **all substantive arguments — technical, constitutional, and evidentiary — will be made by the Petitioner himself.**

4. The Petitioner has formally identified named foreign criminal operators, their data pipeline architecture, and the surveillance infrastructure — in submissions to government bodies, all of which failed to act — and now before this Court. He faces a specific threat environment in consequence. The Petitioner requests a

direction to the Court monitor security for an immediate 48-hour physical and digital threat assessment and protective measures for his family, consistent with *Mahender Chawla v. Union of India* (2019) 14 SCC 615 and the Witness Protection Scheme 2018.

5. That the Applicant has made every effort to comply with all procedural requirements and has paid the applicable court fees or is exempt by virtue of this being a Public Interest Litigation under Article 32 of the Constitution. The Petition raises questions of national importance that require the earliest possible hearing — every 24 hours of delay corresponds to documented, quantifiable harm to Indian citizens as set out in the Synopsis to this Petition.

PRAYER

(a) Permit the Petitioner to appear and argue the present Writ Petition fully in person — on all technical, constitutional, and evidentiary dimensions — under Order IV, Rule 1(c) of the Supreme Court Rules, 2013.

(b) Extend whistleblower-like protections and direct the court monitor security to file a 48-hour threat assessment and provide ongoing security review for my family; and

(c) Pass any other order as this Hon'ble Court deems fit and proper in the interest of justice.

AND FOR THIS ACT OF KINDNESS THE PETITIONER SHALL AS IN DUTY BOUND EVER PRAY.

Filed by:

Nitish Kumar

Petitioner-in-Person
Date: 25-03-2026

IN THE HON'BLE SUPREME COURT OF INDIA

WRIT PETITION (CRIMINAL) NO. _____/2026

PUBLIC INTEREST LITIGATION

UNDER ARTICLE 32 OF THE CONSTITUTION OF INDIA
IN THE MATTER OF
"Nitish Kumar v. Union of India & Ors."

APPLICATION FOR EARLY / URGENT LISTING (Under Order XXXVIII, Supreme Court Rules, 2013 — Urgent Mention)

To, The Hon'ble Chief Justice of India and His Companion Justices of the Hon'ble Supreme Court of India. The Humble Application of the Petitioner Most Respectfully Showeth:

The Petitioner most humbly submits the following grounds for extreme urgency:

GROUND 1 PERSONAL LIBERTY ARTICLE 21 CLASSIFICATION:

EXTREME URGENCY 105 CITIZENS PER HOUR: are subjected to digital arrest — coercive psychological detention without any procedure established by law, lasting up to 26 documented days. Victims are held in psychological captivity using their own stolen Aadhaar-linked biometric data for false credibility. 83 Indian citizens are dead. Rs. 2,140 crores lost in 2024 alone. Source: MHA I4C Annual Report 2024. Each call is an Article 21 violation. 89 This Court's Article 32 jurisdiction to enforce Article 21 is mandatory and non-deferrable.

PERSONAL LIBERTY CLASSIFICATION: Circular dated 29.11.2025, personal liberty matters are listed automatically within two working days. This ground independently satisfies the Circular's personal liberty condition.

GROUND 2 NATIONAL SECURITY DATA SOVEREIGNTY CLASSIFICATION:

EXTREME URGENCY 80 MILLION BIOMETRIC RECORDS: The complete biometric identity profiles — Aadhaar, PAN, facial biometric, bank account, contact network, location history — of 80 million Indian citizens are held on criminal server infrastructure in Shenzhen, China. The principal architect, Zhu Wei alias Jeffrey Zhu, departed India before the LOC was issued and has never faced any court. Section 3(4) of the Extradition Act 1962 as inserted by Act 66 of 1993 read with UNCAC Article 44 has been available as a legal tool since 2011. It has NEVER been invoked. Not once. In 14 years. For any Chinese accused. This is a national digital security emergency.

GROUND 3 — CONSTITUTIONAL EMERGENCY — DPDPA BOARD — CLASSIFICATION: EXTREME URGENCY PARLIAMENT'S MANDATE UNENFORCEABLE:

The Digital Personal Data Protection Act 2023 was enacted by Parliament on 11 August 2023. The Data Protection Board — its enforcement arm — has NOT been constituted for 2 years and 7 months. Not one breach notification has been issued to any of the 80 million affected citizens. 'Shall constitute' is mandatory language. The executive has rendered Parliament's protection mandate wholly inoperative. A writ of mandamus is compelled as a matter of constitutional necessity.

GROUND 4 — IRREVERSIBLE HARM — THE ONE WRONG DECISION

In 2020 the State investigated this ecosystem. It followed the money. It did not follow the data. That single investigative decision made the harm to 80 million citizens permanently irreversible. Money attached under PMLA can be returned — it is reversible harm. An Aadhaar number on a criminal server in Shenzhen cannot be changed. A facial biometric cannot be recalled. A contact list cannot be unexported. Every day without this Court's direction is a day the data is used — right now, at this moment — to generate 105 more

digital arrest calls. This Court's environmental PIL doctrine — M.C. Mehta v. Union of 90 India — recognises that where harm is irreversible, judicial intervention must be at the threshold. That threshold has been exceeded many times over.

GROUND 5 — FRESH CASE — NOT COVERED IN ANY PENDING MATTER

This petition raises six constitutional dimensions not addressed in SMW (Crl.) No. 3 of 2025 or any other pending matter: (i) three-layer data pipeline never forensically investigated; (ii) adtech SDK surveillance — InMobi/Silverpush — never argued before any Indian court; (iii) Section 3(4) Extradition Act 1962 read with UNCAC Article 44 — never invoked for any Chinese accused; (iv) victim profiling — how fraudster knew victim was alone with money and no family calls; (v) Digital Constitutional Personhood — new doctrine under Articles 21, 141, 142; (vi) Root Cause Analysis of existing SOPs — never placed before any court. The Registry is respectfully requested NOT to tag this petition to SMW 3/2025 without the Bench first deciding the distinctness question. OFFICIAL HARM QUANTIFICATION — ALL FIGURES FROM MHA I4C ANNUAL REPORT 2024: Time Unit Documented Harm Nature Every Hour 105 digital arrest calls | Rs. 8.5 crore coerced Article 21 violation — every hour Every Day 2,520 digital arrest calls | Rs. 204 crores coerced Est. 1-2 self-harm incidents Every 48-72 Hours New predatory app re-uploaded — identical architecture, new name Reconstitution cycle — judicial direction needed Each Day Without DPB 80 million breach victims — zero statutory protection Parliament's mandate unenforceable — mandamus compelled Each Day Zhu Wei Is Free Master database of 80M records — access unchallenged Section 3(4) + UNCAC Art.44 available 14 years — never used

GROUND 6 — ADMINISTRATIVE REMEDY COMPLETELY EXHAUSTED

Specific expert intelligence submitted to MeitY, MHA/I4C, RBI, SCI, PMO, and NCSC between 2022 and 2026. Every submission acknowledged. Zero investigative action triggered. Evidence at Annexures P-14 and P-15. No administrative remedy remains. This Court is the only remaining constitutional forum.

PRAYER:

The Petitioner most humbly prays that this Hon'ble Court may be pleased to:

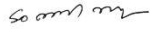
(a). NEXT WORKING DAY LISTING: List this Writ Petition for urgent hearing on the next working day — or within two working days as per the automatic listing mechanism under Circular dated 29.11.2025 for personal liberty matters where defects are cured.

(b). PETITIONER PROTECTION: Direct court monitor security to file 48-hour physical and digital threat assessment and provide appropriate protective measures under Mahender Chawla v. Union of India (2019) 14 SCC 615; and

(c). ANY OTHER ORDER: Pass such other orders as this Hon'ble Court deems fit in the interest of justice and protection of the digital constitutional rights of 80 million+ Indian citizens.

AND FOR THIS ACT OF KINDNESS THE PETITIONER SHALL AS IN DUTY BOUND EVER PRAY.

Nitish Kumar



Petitioner-in-Person
Date: 25-03-2026

IN THE HON'BLE SUPREME COURT OF INDIA

WRIT PETITION (CRIMINAL) NO. _____/2026

PUBLIC INTEREST LITIGATION

UNDER ARTICLE 32 OF THE CONSTITUTION OF INDIA
IN THE MATTER OF
"Nitish Kumar v. Union of India & Ors."

To

The Registrar,

Supreme Court of India,

Tilak Marg, New Delhi – 110 001.

Subject: Letter of Clarification — Maintainability, Locus Standi, Personal Liberty Classification for Listing within Two Working Days under CJI Circular dated 29.11.2025, Distinctness from Earlier Petitions, Evidence Base, Scope of Reliefs, Exhaustion of Remedies, and Prayer for Priority Processing — WP (Criminal) PIL, Nitish Kumar v. Union of India & Ors.

Respected Sir / Ma'am,

I, Nitish Kumar, Petitioner-in-Person and National Cyber Security Scholar under the National Security Database (NSD) Program of Rashtriya Raksha University (an institution established by the Ministry of Home Affairs), most respectfully submit this consolidated Letter of Clarification in response to the Registry's observations and to address all procedural questions regarding the above Writ Petition in one place, so that the matter may be processed and placed before the Hon'ble Court at the earliest.

1. LOCUS STANDI (Maintainability as PIL)

The present Petition is filed purely in public interest and concerns large-scale, ongoing violation of fundamental rights affecting over 80 million Indian citizens. The Petitioner has no personal, financial, or private interest in the outcome. The maintainability of this Petition as a PIL is established on the following grounds:

a) The Petition does not seek any personal relief or private gain for the Petitioner.

b) The issues raised pertain to systemic failures in protection of personal data and cybercrime enforcement at the national level.

c) The affected class comprises ordinary citizens who are either unaware of the violation of their rights, unable to identify the cause, or individually incapable of approaching this Hon'ble Court.

d) The Petitioner has approached all relevant authorities — MeitY, MHA/I4C, RBI, SCI, PMO, and NCSC — between 2022 and 2026 with detailed formal representations. All have been acknowledged. Zero investigative action has resulted. This is documented at Annexures P-14 and P-15 of the Writ Petition.

The bona fide intent of the Petitioner and the exhaustion of all available administrative remedies are thus fully established. Invocation of Article 32 is constitutionally justified.

2. NATURE OF WRIT (Article 32 Jurisdiction)

The present Petition primarily seeks issuance of:

a) Writ of Mandamus — directing Respondent authorities to exercise statutory powers already vested in them under existing laws, specifically Section 3(4) of the Extradition Act 1962 read with UNCAC Article 44,

Section 18 of the DPDPA 2023 (constitution of the Data Protection Board), and Sections 43A and 69A of the Information Technology Act 2000.

b) Writ of Continuing Mandamus — for Court-monitored compliance in a matter involving ongoing, evolving, and technologically complex harm.

c) Appropriate directions under Article 141 & 142 of the Constitution — for effective and complete justice in a transnational matter that existing domestic enforcement mechanisms have been unable to address.

The Petition does not seek formulation of new policy. It seeks enforcement of existing statutory and constitutional obligations that are already vested in the Respondents and have remained unexercised for periods ranging from 2.5 to 12 years.

3. CLARIFICATION ON EVIDENCE BASE

The Petition is not based on speculative or unverified claims. Every factual assertion is anchored to an official, publicly verifiable source:

a) MHA I4C Annual Report 2024 — 105 digital arrest calls per hour; Rs. 2,140 crores lost in 2024; 83+ citizen deaths.

b) NCRB Data — cybercrime case statistics confirming the scale of the problem.

c) Parliamentary Committee Reports — confirming that the DPDPA Data Protection Board has not been constituted.

d) RBI Regulatory Orders — NBFC enforcement and KYC compliance record.

e) FTC Consent Order, Docket C-4530 (2016) — InMobi covert Wi-Fi geolocation surveillance on 100 million devices including children, without consent.

f) FTC Warning Letters, March 2016 — Silverpush ultrasonic audio beacon technology enabling cross-device tracking and microphone access.

g) ED / CBI Court Records — named Chinese accused, LOC issuance dates, and departure timelines.

h) Extradition Act 1962, Section 3(4) as inserted by Act 66 of 1993, and UNCAC Article 44 — statutory texts confirming 14 years of non-invocation.

Independent threat intelligence reports are relied upon only as corroborative material. The primary evidentiary foundation is entirely official. Annexures P-1 to P-17 establish a consistent and traceable evidentiary chain. The Petition is evidence-driven and raises squarely justiciable constitutional questions.

4. SCOPE AND NATURE OF RELIEFS SOUGHT

The reliefs sought in the Petition are structured, specific, and confined to matters within the judicial competence of this Hon'ble Court:

a) Enforcement of existing statutory powers that respondent authorities possess but have not exercised.

b) Investigation and accountability directions — including sworn affidavits from Respondents on six specific factual questions and constitution of a Court-monitored Special Investigation Team.

c) Protection of the fundamental rights of Indian citizens under Articles 14, 19(1)(a), and 21 of the Constitution.

d) Institutional response mechanisms for ongoing, irreversible harm — including direction for constitution of the DPDPA Data Protection Board and invocation of extradition tools.

No relief seeks compensation, policy framing, or any direction outside this Hon'ble Court's constitutional competence. The interim prayers specifically seek sworn

government affidavits disclosing factual information that is exclusively within the Respondents' knowledge.

5. URGENCY AND PERSONAL LIBERTY CLASSIFICATION

The Petitioner respectfully submits that the present matter qualifies for listing within two working days under the personal liberty classification in the CJI Circular dated 29.11.2025, once any Registry-identified defects are cured. This submission is made on the following independent grounds:

(a) 105 Article 21 Violations Per Hour — Present and Continuing. As documented in the MHA I4C Annual Report 2024, 105 Indian citizens per hour are subjected to digital arrest — a form of coercive psychological detention without any procedure established by law, lasting up to 26 documented days per victim — enabled entirely by stolen Aadhaar-linked biometric data. 83 citizens are dead. Rs. 2,140 crores were coercively extracted from victims in 2024 alone. Each such call constitutes a present and ongoing violation of Article 21 of the Constitution against an identifiable, quantifiable citizen.

(b) Personal Liberty Classification Applies to This PIL. The Circular's personal liberty classification is not confined to cases in which the petitioner himself is in custody or detention. Under the ratio of Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1, informational self-determination, bodily integrity, and the right to control one's own biometric data are core components of personal liberty guaranteed under Article 21. Under this Court's well-established expansive PIL jurisdiction under Article 32, the hourly Article 21 violations suffered by 105 identifiable Indian citizens per hour — quantified and documented by the MHA itself — constitute a present, continuing, and mass personal liberty emergency. This

independently and fully satisfies the personal liberty condition in the Circular.

(c) National Security — Independent Urgency Ground. The complete biometric identity profiles of 80 million Indian citizens — Aadhaar numbers, PAN, facial biometrics, bank account details, contact networks, and location histories — are held on criminal server infrastructure in Shenzhen, China, and are being actively weaponised against Indian citizens in real time. The principal architect, Zhu Wei (alias Jeffrey Zhu), departed India before his Look Out Circular was issued and has never faced any Indian court. This constitutes a live, ongoing national digital security emergency, independent of the personal liberty ground.

(d) Irreversibility — Threshold for Judicial Intervention. In M.C. Mehta v. Union of India, this Hon'ble Court established that where harm is irreversible, judicial intervention must occur at the threshold, not after further damage is done. Biometric data permanently exported to foreign criminal infrastructure cannot be recalled by any domestic order. Every day of delay is a day that data is being used — right now, at this moment — to generate 105 more digital arrest calls against Indian citizens. The threshold for judicial intervention was crossed long ago.

(e) The Matter Involves Continuing Harm of an Irreversible Nature. The harm in this Petition is not historical — it is happening at this moment. Ongoing misuse of biometric data at scale, harm that cannot be reversed once biometric data is compromised, and continuous re-constitution of predatory applications confirm that delay in adjudication directly and measurably increases irreparable harm.

(f) Defect Cure Undertaking. The Petitioner undertakes to cure any Registry-identified defect within 24 hours of communication and respectfully requests

that the two-working-day listing clock under the CJI Circular dated 29.11.2025 be reckoned from the date on which defects are certified as cured.

6. CLARIFICATION FROM OTHER MATTERS

The present Petition raises specific constitutional and factual questions not covered in any pending proceeding, including SMW (Crl.) No. 3 of 2025. The distinction is not one of degree but of subject matter:

a) Every existing proceeding has followed the money trail. The present Petition follows the data trail — a dimension that has never been investigated or adjudicated.

b) The three-layer data pipeline — AdTech surveillance SDKs (InMobi / Silverpush), defaulter NBFC KYC collection, and Chinese-controlled backend aggregation — is identified here for the first time in any judicial proceeding.

c) The 14-year non-invocation of Section 3(4) of the Extradition Act 1962 against named Chinese principals has never been placed before any court.

d) The non-constitution of the DPDPA 2023 Data Protection Board for 2 years and 7 months, rendering Parliament's mandate wholly unenforceable, is raised as a standalone mandamus ground for the first time.

e) The constitutional doctrine of Digital Personhood under Article 21 in the AI era, and the State's affirmative obligation to seek forensic destruction of exfiltrated citizen data from foreign criminal servers, is raised for the first time before this Court.

The Registry is respectfully requested not to tag or club the present Petition with SMW (Crl.) No. 3 of 2025 or any other matter without first placing the question of distinctness before the Bench. The Petitioner submits that mechanical clubbing would result in these novel constitutional questions never being examined and

would itself constitute a denial of justice to the 80 million citizens on whose behalf this Petition is filed.

7. EXHAUSTION OF REMEDIES

The Petitioner has, over a period of four years from 2022 to 2026, submitted detailed formal representations to MeitY, MHA/I4C, RBI, SCI, PMO, and NCSC — setting out the precise facts, the data pipeline architecture, the named accused, and the statutory tools available for action. Every submission has been acknowledged in writing. Not one has resulted in investigative action. This is evidenced at Annexures P-14 and P-15 of the Writ Petition. There is no administrative remedy remaining. This Hon'ble Court under Article 32 is the only remaining constitutional forum.

8. NOTE FOR THE REGISTRY — PARAGRAPH TO BE FORWARDED WITH THE MATTER

The Petitioner respectfully requests that the following paragraph be noted and, if appropriate, forwarded along with the matter to the Hon'ble Court:

> *In 2020 the State investigated this ecosystem. It followed the money. It should have followed the data. That one decision made the harm to 80 million Indian citizens permanently irreversible. The Aadhaar numbers, facial biometrics, contact lists, and location histories on criminal servers in Shenzhen cannot be changed, recalled, or deleted by any domestic court order. They are being used right now — at this moment — to generate 105 digital arrest calls per hour against identifiable Indian citizens. 14 years of available extradition tools — Section 3(4) and UNCAC Article 44 — were never used. 2.5 years of Parliament's data protection mandate — DPDPA 2023 — is unenforceable because the Board was never constituted. 83+ citizens are dead. Rs. 52,000 crores has been lost. This petition asks this Court to do what five years of administrative action has not done: follow*

the data, extradite the architects, and declare the digital constitutional personhood of Indian citizens as a protected fundamental right in the AI era. That is why this petition must be listed within two working days. Not as procedural courtesy — as constitutional necessity.

9. PRAYER FOR EARLY LISTING

In view of all of the above, it is most respectfully prayed that the Registry may be pleased to:

a). Process this Writ Petition under the personal liberty / national security classification of the CJI Circular dated 29.11.2025 and list it before the appropriate Bench within two working days of the cure of any defects;

b). Not tag, club, or amalgamate this Petition with SMW (Crl.) No. 3 of 2025 or any other pending matter without first placing the question of distinctness before the Hon'ble Bench;

(c).Communicate any Registry defects to the Petitioner at nkumar906099@gmail.com or +91-9082843142 at the earliest so that the same may be cured within 24 hours; and

(d). Process this Petition on priority, noting that it is evidence-backed, filed in strict good faith, raises substantial questions of national constitutional importance not covered in any pending matter, and documents a present, hourly, quantifiable emergency that permanently worsens with every day of delay.

Yours faithfully,

Nitish Kumar

Petitioner-in-Person
Date: 25-03-2026

IN THE HON'BLE SUPREME COURT OF INDIA

WRIT PETITION (CRIMINAL) NO. _____/2026

PUBLIC INTEREST LITIGATION

UNDER ARTICLE 32 OF THE CONSTITUTION OF INDIA
IN THE MATTER OF
"Nitish Kumar v. Union of India & Ors."

FILING INDEX

S.NO	PARTICULARS OF DOCUMENTS FILED	COPIES	COURT FEES PAID
1.	Synopsis and list of dates	B-H	
2.	Writ petition with affidavit	1-39	
3.	Appendix copy of article 136 of constitution of India	40 -46	
4.	Annexure P-1 to P-17	47 to 113	
5.	Application for permission to appear and argue in person	114-116	
6.	Application for early / urgent listing	117-120	
7.	Letter to Registrar	121-129	
8.	Filing index	130-131	
9.	Memo of appearance	132	
10.	Declaration	133	

Court Fee: Exempted (Public Interest Litigation under Article 32)

Filed by:

Nitish Kumar

Petitioner-in-Person
Date: 25-03-2026

IN THE HON'BLE SUPREME COURT OF INDIA

WRIT PETITION (CRIMINAL) NO. _____/2026

PUBLIC INTEREST LITIGATION

UNDER ARTICLE 32 OF THE CONSTITUTION OF INDIA
IN THE MATTER OF
"Nitish Kumar v. Union of India & Ors."

MEMO OF APPEARANCE

To,

The Registrar,

Hon'ble Supreme Court of India,

Tilak Marg, New Delhi – 110 001.

Sir / Ma'am,

Kindly enter my appearance in person for the above-named Petitioner in the captioned matter.

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, the Petitioner-in-Person in the above matter, hereby enter my appearance and request that all notices, communications, and orders in the captioned matter may be served on me at the following address:

Yours faithfully,

Nitish Kumar

Petitioner-in-Person
Date: 25-03-2026

DIARY NO: 20329 OF 2026

REFILING DECLARATION

DIARY NO: 20329 OF 2026

DECLARATION

All the defects have been duly cured. Whatever has been added/deleted/modified in the petition is the result of curing of the defects and nothing else. Except curing the defects, nothing has been done. Paper books are complete in all respects.

Filed by:

Nitish Kumar

Petitioner-in-Person
Date: 25-04-2026

ID

भारत गणराज्य REPUBLIC OF INDIA

P IND T7115700

NITISH KUMAR

भारतीय/INDIAN M 18/01/1993

JHAJHA,BIHAR

PATNA

14/11/2019 13/11/2029

P<IND<<NITISH<KUMAR<<<<<<<<<<<<<<<<<<<<<<<<<<<<

T7115700<4IND9301180M2911135<<<<<<<<<<<<<<<2

T7115700

DILIP KUMAR

ANITA BALA

VILL ALKJARA NH333 JHAJHA

JHAJHA,JAMUI

PIN:811308,BIHAR,INDIA

PA27C4097486619