NITISH KUMAR

National Cyber Security Scholar

Rashtriya Raksha University

D2–8206, Eco Floors, Kharar–Mohali, Punjab – 140 301

nkumar906099@gmail.com | +91-9082843142

Date of Submission:	20 May 2026
Category:	National Security / Cybersecurity / Data Protection / Judicial Direction
Sub-Category:	Supreme Court Directed Representation — Non-action by Ministry
Submitted by:	Nitish Kumar, National Cyber Security Scholar, RRU
Contact:	nkumar906099@gmail.com | +91-9082843142 | D2-8206 Eco Floors, Kharar–Mohali, Punjab – 140 301
Ministry Concerned:	Ministry of Electronics and Information Technology (MeitY)
Copy to:	National Security Advisor | CERT-In | I4C/MHA | NCSC
Related Case:	Nitish Kumar v. Union of India & Ors. — W.P.(Crl.) No. 163/2026 — Supreme Court of India
SC Order Date:	19 May 2026 — CJI Surya Kant, J. Bagchi, J. Pancholi — Direction to MeitY & cyber agencies

SUBJECT: PUBLIC GRIEVANCE AND NATIONAL SECURITY ALERT — pursuant to the direction of the Hon'ble Supreme Court of India in *Nitish Kumar v. Union of India & Ors.* [W.P.(Crl.) No. 163/2026] dated 19 May 2026 — directing MeitY and relevant cyber security agencies to examine a formal representation regarding (a) the systematic exfiltration of biometric and personal data of 80 million+ Indian citizens to Chinese-controlled servers; (b) an imminent, time-specific, multi-vector cyber-financial attack on India's banking infrastructure expected in June, September, and October 2026 by entities coordinating from China, Cambodia/UAE, and domestic staging nodes in Nepal, Jamtara, Asansol, and Patna; and (c) the non-operationalisation of the Digital Personal Data Protection Act 2023 — requesting the Prime Minister's Office to route this grievance to MeitY, the National Security Advisor, and CERT-In for immediate, time-bound action, as the nation has very limited time to act.

1. This grievance is submitted pursuant to the direction of the Hon'ble Supreme Court of India issued on **19 May 2026** by a three-judge bench comprising the Chief Justice of India, Hon'ble Mr. Justice Surya Kant, Hon'ble Mr. Justice Joymalya Bagchi, and Hon'ble Mr. Justice Vipul M. Pancholi, in *Nitish Kumar v. Union of India & Ors.* [W.P.(Crl.) No. 163/2026]. The Hon'ble Court directed as follows:

> *"The issues sought to be raised by the petitioner being highly technical in nature...it seems to us that the appropriate representation for a digital approach should be made to the Ministry of Electronics and Information Technology (MeitY), information security, and cyber agencies. Let this plea be given as a supplementary representation. They shall consider it."*
>
> **— Chief Justice of India Surya Kant | W.P.(Crl.) No. 163/2026 | 19 May 2026**

The petition has been submitted to MeitY and CERT-In on 20 May 2026. This PMOPG grievance is filed simultaneously to ensure the Prime Minister's Office is on formal notice and can route this matter for immediate action, as the Supreme Court's direction carries a governmental obligation for time-bound

consideration. The proof of service of the MeitY submission, the AG/SG communication, and this grievance are being dispatched by Speed Post today and will be attached as proof of delivery upon receipt.

2. I am Nitish Kumar, a National Cyber Security Scholar from Rashtriya Raksha University, functioning under the Ministry of Home Affairs, Government of India. I have been independently monitoring, documenting, and reporting on a state-linked Chinese cyber-financial threat ecosystem operating against India since 2022. I am not affiliated with any political party. I am not on social media. I hold approximately **6,000 pages of documented evidence** on this ecosystem. I have submitted intelligence to MeitY, I4C/MHA, RBI, PMO, and the National Cyber Security Coordinator between 2022 and 2025. Every submission received either a standard acknowledgement or no response. I went to the Supreme Court of India as the last constitutional resort. The Court has now directed the executive to act. I am filing this grievance because **the nation has very limited days remaining to prevent an irreversible harm** and every channel must be on record.

3. The following matters are formally placed before the Prime Minister's Office:

- Systematic exfiltration of biometric and personal data — Aadhaar, PAN, facial biometrics, SMS records, bank account data — of 80 million+ Indian citizens to Chinese-controlled servers between 2017 and 2022, through predatory loan applications (CashBean, RupeeLend, MiCredit and 400+ others), shell NBFC KYC collection fronts (Cred Fintech Pvt Ltd, Acemoney India Ltd, Transerve Technologies, HiWe Finance), and adtech SDK covert surveillance (InMobi — US FTC Consent Order 2016; Silverpush — FTC Warning Letters 2016).
- Named principal Chinese architects — Jeffrey Zhu (Zhu Wei), Liu Yang, Zhuang Wei, Wang Xin, Chen Wei — none of whom have faced any court in any jurisdiction. India has filed zero extradition requests against any named Chinese principal, despite Section 3(4) of the Extradition Act 1962 read with UNCAC Article 44 providing the exact legal mechanism since 2011. This tool has never been used.
- Non-operationalisation of the Digital Personal Data Protection Act 2023 (enacted August 2023) and non-constitution of the Data Protection Board — leaving 80 million affected citizens with no statutory enforcement forum as of 20 May 2026.
- Documented consequence at national scale: ₹1.5 lakh crore in digital fraud losses through 2026; 105 Indian citizens subjected to digital arrest every hour; 83+ deaths by suicide; 8 billion potential fraudulent operations.
- Five years of representations to MeitY, I4C/MHA, RBI, PMO, and NCSC — all unacted upon — evidenced at Annexures P-14 and P-15 of the Writ Petition. This PMOPG grievance continues that chain and is being preserved as evidence.

ANTICIPATORY INTELLIGENCE SUBMISSION — HIGHEST URGENCY

IMMINENT CYBER-FINANCIAL ATTACK ON INDIA: JUNE / SEPTEMBER / OCTOBER 2026

This intelligence has been submitted to MeitY and CERT-In on 20 May 2026, to the Attorney General and Solicitor General of India by Speed Post on 20 May 2026, and is now formally placed before the Prime Minister's Office. It is submitted as anticipatory intelligence — verifiable, documented, and time-specific. The nation has weeks, not months, to act on the June window.

4. On the basis of five years of independent intelligence monitoring and pattern analysis of the Chinese-directed cyber-financial ecosystem operating in India, the Petitioner submits the following anticipatory intelligence:

- Approximately 2 lakh (200,000) corporate and merchant bank accounts across India have been compromised and staged — placed under foreign-directed operational control without the account holders' knowledge — and are being held in reserve for simultaneous activation. These are legitimate business accounts, not newly opened mule accounts.
- The command architecture coordinates primarily from China (Shenzhen and Hong Kong server clusters) — the same infrastructure that received the 2020 exfiltration of 80 million Indian

biometric records, which is still operationally active. Intermediate coordination nodes are in Cambodia and UAE.

- Domestic last-mile execution is staged through networks in Nepal, Jamtara (Jharkhand), Asansol (West Bengal), Patna (Bihar), and associated state-level networks. These are not independent criminal cells — they are coordinated nodes in a single foreign-directed command structure.
- Primary execution window: June 2026. Escalation windows: September and October 2026 — timed to correspond with the Navratri and Diwali festival season payment volumes, when transaction scrutiny is reduced and institutional vigilance is typically lower.
- The attack mechanism: simultaneous activation of the 2 lakh staged accounts for high-value transfers; combined with AI-driven digital arrest operations targeting company principals using 80 million biometric records already held on Chinese servers; combined with UPI and payment gateway manipulation — all designed to execute faster than law enforcement response capacity.
- The threat is not confined to financial loss. It is structured to create a systemic confidence crisis in India's banking and digital payment infrastructure in the months before a major political and economic season. This constitutes a cyber-economic warfare operation directed at the stability of the present Government and the financial security of the nation.

5. This is not the first time this intelligence has been placed before the Government. The following submissions were made and are evidenced by postal receipts and portal acknowledgements attached as proof of service:

- MeitY — multiple representations by registered post and grievance portal, 2022–2025. Outcome: standard acknowledgement; no investigative action.
- I4C/MHA (Indian Cyber Crime Coordination Centre) — intelligence submissions on predatory loan app architecture and Chinese principal architects. Outcome: no action.
- Reserve Bank of India — submissions on shell NBFC KYC data collection fronts. Outcome: no action.
- Prime Minister's Office (PMO) — grievance submissions 2022–2025. Outcome: forwarded to MeitY; standard acknowledgement only.
- National Cyber Security Coordinator's Office — direct submissions. Outcome: no response.

The Supreme Court of India, on 19 May 2026, heard this matter and directed MeitY and relevant cyber security agencies to examine the petition as a formal representation for **deep, time-bound consideration.** This PMOPG grievance is filed on the same day as the MeitY submission to ensure the Prime Minister's Office has a complete, parallel record and can direct immediate action. The grievance is being preserved as legal evidence of the Government's knowledge of this threat as of 20 May 2026.

6. The Supreme Court's direction of 19 May 2026 is a matter of national public record, having been reported by the Press Trust of India (PTI) wire across 11 confirmed national and regional publications including Verdictum, The Tribune, Deccan Chronicle, The Federal, Madhyamam Online, OrissaPOST, Telangana Today, and Communications Today. The PTI wire network reaches 500+ subscriber outlets. This matter cannot be routed for routine closure — it carries judicial imprimatur, national media record, and active security intelligence.

7. The Petitioner respectfully requests the Prime Minister's Office to take the following actions:

- Route this grievance immediately to MeitY (Secretary-level), the National Security Advisor, the National Cyber Security Coordinator, and CERT-In as a priority national security matter — not as a routine ministerial referral.
- Ensure MeitY issues a substantive, time-bound response to the Supplementary Representation filed on 20 May 2026 pursuant to the Supreme Court's direction, within the six-week window before contempt proceedings become necessary.
- Direct the National Security Advisor to examine the anticipatory intelligence on the June, September, and October 2026 cyber-financial attack windows and initiate immediate preventive action on the 2 lakh staged corporate and merchant accounts.
- Direct the constitution of the Data Protection Board under the DPDPA 2023 without further delay — the statutory framework exists but has not been activated, leaving 80 million citizens with no protection or remedy.

- Direct CERT-In and I4C/MHA to initiate a coordinated forensic investigation specifically targeting the data pipeline and backend server infrastructure — not only money flows — and to provide a report to the NSA within 30 days.
- Note formally that if no substantive action is taken by 30 June 2026, the Petitioner will file contempt of court proceedings before the Supreme Court upon resumption after the vacation period. The PM's Office is being placed on notice of this timeline today.

I have brought this matter to every door available to a citizen of India — administrative, regulatory, judicial, and now directly to the Prime Minister's Office. I have no personal interest in any outcome except that 80 million of my fellow citizens are protected and that the nation I serve is not destroyed by a foreign-directed cyber-economic attack in the months ahead. The Supreme Court of India has spoken. The direction is clear. I respectfully ask that the Prime Minister's Office ensure that direction is honoured — not for my sake, but for the nation's.

Yours faithfully,

s/d

NITISH KUMAR
National Cyber Security Scholar
Rashtriya Raksha University (Ministry of Home Affairs, Government of India)
Petitioner-in-Person | W.P.(Crl.) No. 163/2026 | Supreme Court of India
Date: 20 May 2026 | Place: Chandigarh, Punjab

PROOF OF SERVICE AND ENCLOSURES:

- Enclosure 1 — Writ Petition (Criminal) — Nitish Kumar v. Union of India & Ors. [W.P.(Crl.) No. 163/2026] — Complete petition (WRIT_V6) — the substantive representation to MeitY [TO BE ATTACHED]
- Enclosure 2 — Supplementary Representation Cover Letter to MeitY Secretary and CERT-In DG dated 20 May 2026 [ATTACHED]
- Enclosure 3 — Technical Intelligence Report: Indian Adtech and SDK Ecosystem — Privacy Risks, Surveillance Infrastructure, and Regulatory Gaps 2012–2026 [ATTACHED]
- Enclosure 4 — Communication to Attorney General and Solicitor General of India dated 20 May 2026 [ATTACHED]
- Enclosure 5 — National Media Coverage Log — 11 confirmed listings (Verdictum, PTI, The Tribune, Deccan Chronicle, The Federal, Madhyamam Online, OrissaPOST, Telangana Today, Communications Today, NewsDrum, Lawstreet Journal) [ATTACHED]
- Enclosure 6 — Speed Post receipts / proof of delivery for MeitY submission and AG/SG communication [TO BE ATTACHED UPON RECEIPT]
- Enclosure 7 — Prior representations to MeitY, I4C/MHA, RBI, PMO, NCSC (2022–2025) with postal receipts and portal acknowledgements [ATTACHED — Annexures P-14 and P-15 of Writ Petition]

NOTE ON ROUTING — FOR PMOPG GRIEVANCE OFFICER:

This grievance is filed under the Citizens Charter and Grievances (CPGRAMS / PGPORTAL) framework. It concerns a matter of national security with a time-specific threat window. It MUST NOT be routed for closure as a standard ministry referral. Under the Allocation of Business Rules 1961 and the Government of India (Transaction of Business) Rules 1961, matters involving national security are to be brought to the attention of the Prime Minister directly where the information warrants it. This grievance contains anticipatory intelligence of a foreign-directed attack on India's banking infrastructure scheduled for June–October 2026. It should be routed simultaneously to: (1) MeitY — for action on the SC-directed representation; (2) PMO Security Cell / NSA Office — for the anticipatory intelligence; (3) CERT-In — for immediate technical action; (4) I4C/MHA — for coordinated law enforcement response. Proof of routing must be communicated to the petitioner at the contact details above.

Legal basis for priority routing: Section 4(1)(c) of the RTI Act 2005 (proactive disclosure obligation for matters affecting national interest); PGPORTAL Grievance Redressal Guidelines 2023 (time-bound disposal for security-classified matters); Supreme Court direction in W.P.(Crl.) No. 163/2026 dt. 19.05.2026 (binding direction to consider as formal representation).

This grievance is filed in the national interest. It is preserved as evidence of the Government's knowledge of the matters stated herein as of 20 May 2026.

Gmail

Nitish Kumar <nkumar906099@gmail.com>

Supplementary Representation pursuant to the direction of the Hon'ble Supreme Court of India in Nitish Kumar v. Union of India & Ors. [W.P.(Crl.) No. 163/2026] — Order dated 19 May 2026 — forwarding the Writ Petition as a formal representation to MeitY and relevant cyber security agencies for time-bound consideration, along with a compilation of national media coverage confirming the matter of public record.

1 message

Nitish Kumar <nkumar906099@gmail.com> Wed, May 20, 2026 at 5:03 PM
To: moeit@gov.in, mos-eit@gov.in, kshitij.singha@gov.in, secretary@meity.gov.in
Cc: hshso@nic.in, sois-mha@nic.in, pmo@gov.in, connect@mygov.nic.in, secretary@meity.gov.in, cert-in@nic.in, incident@cert-in.org.in, cybercrime@i4c.gov.in, grievance-pg@nic.in, ps2pm@nic.in, cabsec@nic.in, ceo-i4c@mha.gov.in

Respected Sir / Ma'am,

1. I write to you in direct compliance with and pursuant to a formal direction issued by the Hon'ble Supreme Court of India on **19 May 2026** by a bench comprising the Chief Justice of India, Hon'ble Mr. Justice Surya Kant, Hon'ble Mr. Justice Joymalya Bagchi, and Hon'ble Mr. Justice Vipul M. Pancholi, in ***Nitish Kumar v. Union of India & Ors.*** [W.P.(Crl.) No. 163/2026].

> *"The issues sought to be raised by the petitioner being highly technical in nature, with a very limited legal regime being involved and hardly any significant legal issue present, it seems to us that the appropriate representation for a digital approach should be made to the Ministry of Electronics and Information Technology (MeitY), information security, and cyber agencies. Let this plea be given as a supplementary representation. They shall consider it."*
>
> **— Chief Justice of India Surya Kant, 19 May 2026 | W.P.(Crl.) No. 163/2026**

2. The Hon'ble Court disposed of the Writ Petition, directing that it be treated as a formal supplementary representation forwarded to MeitY and relevant cyber security agencies for **deep, time-bound consideration.** Accordingly, **the complete Writ Petition (WRIT_V6) is attached to this letter as the substantive submission.** This Ministry is respectfully requested to treat the attached petition document — containing the full factual record, constitutional arguments, intelligence submissions, technical evidence, and reliefs sought — as the primary representation. This covering letter serves only to formally place the petition before this Ministry pursuant to the Supreme Court's direction.

> *This is an anticipatory submission regarding an imminent, time-specific cyber-financial threat to India's banking infrastructure expected in June, September, and October 2026. The threat originates from entities coordinating across China, Cambodia/UAE (especially Pakistan, which is highly sensitive), with weaponization anticipated in September and October 2026. Domestic staging nodes include Nepal, Jamtara, Asansol, Patna, and associated networks, involving an estimated 2 lakh corporate and merchant accounts already staged for simultaneous activation. I have provided 4 accounts detailing exactly what they do. Chien Wie, also known as James Wei, is extradited to China in January 2026 with all C2 servers where Indian live feed data is present. As you read this, everything in the nation is bugged; when I say everything, I mean everything. There is no privacy because malware is in the hardware, and no software can clean that yet. Sit silent, as no one can capture. This has made me seriously concerned that the nation faces an extreme risk of the present government falling and national destruction, which I will not allow. This submission is entirely for my nation and I look forward to a meeting. We must immediately ban the adtech firm (Silverpush and InMobi, partnered with Apsus from China) mentioned in the attached file [* **Intelligence report.pdf** *] . At least, interim demand by the nation where we are already sharing evidence, and i would be sharing it with the PM and NSA by Speedpost. I*

> *am sending this to the BJP chief for information, and the same to Congress , as this is all about my nation which comes first for me. There are approximately 6,000 pages of evidence detailing the crime and types they would do. Even following standard operating procedure (SOP), it cannot be stopped because malware resides on the hardware across all offices, leading to a national data breach.*

3. For the Ministry's reference, the attached petition documents the following:

- The systematic exfiltration of biometric and personal data of 80 million+ Indian citizens to Chinese servers between 2017 and 2022, through three documented technical channels — predatory loan applications, shell NBFC KYC collection fronts, and adtech SDK surveillance (InMobi and Silverpush).
- The principal Chinese architects of this operation, including Jeffrey Zhu (Zhu Wei), Liu Yang, Zhuang Wei, Wang Xin, and Chen Wei — none of whom have faced any court in any jurisdiction — and the legal basis for extradition available to India since 1993 through Section 3(4) of the Extradition Act 1962 read with UNCAC Article 44 and UNTOC, which has never been invoked.
- The non-operationalisation of the Digital Personal Data Protection Act 2023 and the non-constitution of the Data Protection Board, leaving 80 million affected citizens without statutory remedy.
- Documented harm: ₹1.5 lakh crore in digital fraud losses; 105 digital arrests per hour; 83+ deaths by suicide; 8 billion potential fraudulent operations arising from 80 million compromised records.
- Five years of intelligence submissions to MeitY, I4C/MHA, RBI, PMO, and NCSC — all unacted upon — attached as Annexures P-14 and P-15.

4. I respectfully wish to place on record that this is not my first submission to this Ministry or to the Government of India on these matters. Representations have been made repeatedly — by registered post and through official grievance portals — to MeitY, I4C/MHA, RBI, PMO, and the National Cyber Security Coordinator's Office between 2022 and 2025. Every submission received either a standard acknowledgement or no response. No investigative action was triggered on any representation. Having exhausted every available administrative channel, I filed the above Writ Petition before the Supreme Court of India as the only remaining constitutional forum for the 80 million citizens whose data rights are being violated daily. The Hon'ble Court has now directed this Ministry to act. I respectfully request that this representation be treated with the urgency required by the Supreme Court's direction and the gravity of the harm.

5. The Supreme Court's direction of 19 May 2026 has been reported by the Press Trust of India (PTI) wire and independently by multiple national and regional publications, confirming this matter is a matter of national public record. The following 11 confirmed listings are provided for this Ministry's reference:

#	Outlet	Category	Headline / URL
1	**Verdictum**	Legal / SC specialist	*Supreme Court Asks Centre To Examine Cyber Security Consultant's Plea For Protection, Recovery & Destruction Of Stolen Personal Data Of Indian Citizens* verdictum.in/supreme-court/cyber-security-consultant-plea-destruction-stolen-personal-data-indian-citizens-1614263
2	**PTI — Press Trust of India**	Primary wire agency	*SC asks MeitY to examine PIL seeking recovery or destruction of stolen personal data of citizens* [Wire dispatch — source for listings 3–9 below]
3	**The Tribune**	National daily (North India)	*Examine PIL on stolen data of citizens, Supreme Court directs Ministry of Electronics and IT* tribuneindia.com/news/india/examine-pil-on-stolen-data-of-citizens-supreme-court-directs-ministry-of-electronics-and-it
4	**Deccan Chronicle**	National daily — legal section	*SC Asks MeitY to Examine Plea on Indians' Stolen Data on Foreign Servers*

			deccanchronicle.com/legalnews/sc-asks-meity-to-examine-plea-on-indians-stolen-data-on-foreign-servers-1957706
5	**The Federal**	National independent	*SC directs MeitY to examine plea on safeguarding Indians' stolen data* thefederal.com/category/news/sc-directs-meity-to-examine-plea-on-safeguarding-indians-stolen-data-243693
6	**Madhyamam Online**	Kerala daily — English edition	*SC asks MeitY to review PIL on stolen personal data of citizens* madhyamamonline.com/india/sc-asks-meity-to-review-pil-on-stolen-personal-data-of-citizens-1521294
7	**OrissaPOST**	Regional daily (Odisha)	*Supreme Court of India asks MeitY to examine plea on stolen personal data* orissapost.com/supreme-court-of-india-asks-meity-to-examine-plea-on-stolen-personal-data
8	**Communications Today**	IT & Telecom trade media	*SC asks MeitY to examine plea on stolen personal data stored abroad* communicationstoday.co.in/sc-asks-meity-to-examine-plea-on-stolen-personal-data-stored-abroad
9	**NewsDrum**	PTI syndication	*SC asks MeitY to examine PIL seeking recovery or destruction of stolen personal data of citizens* newsdrum.in/national/sc-asks-meity-to-examine-pil-seeking-recovery-or-destruction-of-stolen-personal-data-of-citizens-11850558
10	**Lawstreet Journal**	Legal media — cyber beat	*SC / cyber fraud coverage — active beat rotation* lawstreet.co/latest-news/cyber-fraud

Note: The PTI wire network reaches 500+ subscriber outlets across India. The above 11 are independently confirmed listings. Total ecosystem reach estimated at 50–100+ publications within 24 hours of wire dispatch.

6. I respectfully request that this Ministry and CERT-In examine the attached Writ Petition as a formal supplementary representation per the Hon'ble Supreme Court's direction and issue a time-bound response to the Petitioner at the contact details above. I am available to present the technical evidence and intelligence submissions in person or in writing at any time convenient to this Ministry.

This submission is made in the interest of the nation, without any personal motive, and with the full confidence that this Ministry, now formally directed by the Supreme Court of India, will act with the urgency this matter demands.

Nitish Kumar

AI SCHOLAR | DATA SCIENTIST|NATIONAL CYBER SECURITY SCHOLAR -NSD

email: nitish.kumar40@outlook.com |**Mobile:**9082843142

Avoid Corruption! Avoid Racism

---

5 attachments

WRIT V6.pdf
3898K

EASCIN01041492026_FILE_ADDITIONAL_DOCUMENTSFACTSANNEXURES.pdf
4128K

Report as of 2026.pdf
845K

Digital-Crime-Architecture.pptx
271K

Intillgence report.pdf
5920K

Gmail

Nitish Kumar <nkumar906099@gmail.com>

Urgent communication to the Law Officers of the Union of India — informing of (a) the Supreme Court's direction dated 19 May 2026 in Nitish Kumar v. Union of India & Ors. [W.P.(Crl.) No. 163/2026] directing MeitY and relevant cyber security agencies to examine the petition as a formal supplementary representation; (b) an anticipatory submission regarding an imminent multi-vector cyber-financial and national security threat by entities coordinating from foreign jurisdictions, expected to execute in September and October 2026; and (c) respectful notice that if MeitY fails to respond within 6 or 8 weeks of the Court's direction, the Petitioner will move for contempt of court proceedings before the Supreme Court upon resumption after the vacation period — inviting the Law Officers' proactive engagement with the Government in the national interest.

1 message

Nitish Kumar <nkumar906099@gmail.com> Wed, May 20, 2026 at 6:23 PM
To: attorney-general@gov.in, m.nagasubrahmanyam@gov.in, "TUSHAR MEHTA, Solicitor General of India" <tusharmehta.sg@gmail.com>, manish.malhotra@nic.in
Cc: lawofficers-dla@nic.in

Respected Sir,

1. I am Nitish Kumar, a National Cyber Security Scholar from Rashtriya Raksha University, an institution functioning under the Ministry of Home Affairs, Government of India. I am the Petitioner-in-Person in ***Nitish Kumar v. Union of India & Ors.*** [W.P.(Crl.) No. 163/2026], a Writ Petition (Criminal) filed under Article 32 of the Constitution of India before the Supreme Court of India. I write to both Law Officers of the Union not as an adversary of the Government, but as a citizen who has exhausted every administrative door and who now stands before you with verified intelligence of threats to this nation that I believe you, as Law Officers who stand for the Government and for the people it governs, must be made aware of directly.

2. On **19 May 2026**, a three-judge bench of the Supreme Court of India comprising the Chief Justice of India, Hon'ble Mr. Justice Surya Kant, Hon'ble Mr. Justice Joymalya Bagchi, and Hon'ble Mr. Justice Vipul M. Pancholi heard the above Writ Petition. The Hon'ble bench was pleased to direct as follows:

> *"The issues sought to be raised by the petitioner being highly technical in nature, with a very limited legal regime being involved and hardly any significant legal issue present, it seems to us that the appropriate representation for a digital approach should be made to the Ministry of Electronics and Information Technology (MeitY), information security, and cyber agencies. Let this plea be given as a supplementary representation. They shall consider it."*
>
> **— Chief Justice of India Surya Kant | W.P.(Crl.) No. 163/2026 | 19 May 2026**

The Court accordingly disposed of the Writ Petition, directing that the petition be treated as a formal supplementary representation to MeitY and relevant cyber security agencies for **deep, time-bound consideration.** The petition has been submitted to MeitY and CERT-In on 20 May 2026. This direction creates a formal governmental obligation, arising from the order of a three-judge bench led by the Chief Justice of India, that MeitY must examine and respond to within a reasonable and time-bound period.

3. This matter is a matter of national public record. The Supreme Court's direction of 19 May 2026 has been reported by the **Press Trust of India (PTI) wire** and confirmed across **11 national and regional publications** including Verdictum, The Tribune, Deccan Chronicle, The Federal, Madhyamam Online, OrissaPOST, Telangana Today, Communications Today, and NewsDrum. The PTI wire network reaches 500+ subscriber outlets across India. The matter cannot be characterised as a routine grievance — it has judicial imprimatur and national media record.

4. For the Law Officers' reference, the petition concerns the following verified matters of national security:

- The systematic exfiltration of biometric and personal data of 80 million+ Indian citizens — Aadhaar, PAN, facial biometrics, SMS records, bank data — to Chinese-controlled servers between 2017 and 2022, through predatory loan applications, shell NBFC KYC collection fronts, and adtech SDK covert surveillance (InMobi: FTC Consent Order 2016; Silverpush: FTC Warning Letters 2016).
- Named principal Chinese architects — Jeffrey Zhu (Zhu Wei), Liu Yang, Zhuang Wei, Wang Xin, and Chen Wei — none of whom have faced any court in any jurisdiction, and India's documented failure for 14 years to invoke Section 3(4) of the Extradition Act 1962 read with UNCAC Article 44 (available since 2011) to pursue their extradition.
- The non-operationalisation of the Digital Personal Data Protection Act 2023 — in force since August 2023 — and the non-constitution of the Data Protection Board, leaving 80 million affected citizens without any statutory enforcement forum.
- Documented harm at national scale: ₹1.5 lakh crore in digital fraud losses; 105 Indian citizens subjected to digital arrest every hour; 83+ deaths by suicide linked to this ecosystem; 8 billion potential fraudulent operations.
- Five years of intelligence submissions to MeitY, I4C/MHA, RBI, PMO, and NCSC — all unacted upon — evidenced at Annexures P-14 and P-15 of the petition.

5. I must now place before both Law Officers an anticipatory submission of the highest urgency. Based on independent intelligence monitoring and five years of sustained investigative engagement with this ecosystem, I submit that India faces a **planned, coordinated, multi-vector cyber-financial and destabilisation operation** by entities coordinating across foreign jurisdictions, with the primary execution window in **September and October 2026.**

The threat architecture, as documented and submitted to MeitY, is as follows:

- Approximately 2 lakh (200,000) corporate and merchant bank accounts across India have already been staged — compromised and placed under foreign-directed operational control — without the knowledge of the account holders. These are not newly opened mule accounts. They are legitimate business accounts held in reserve for simultaneous activation.
- The coordination originates primarily from China (Shenzhen/Hong Kong server clusters), with intermediate nodes in Cambodia and UAE. The same infrastructure that received the 2020 exfiltration of 80 million biometric records is still operationally active.
- Domestic last-mile execution is being staged through networks in Nepal, Jamtara (Jharkhand), Asansol (West Bengal), Patna (Bihar), and associated networks. These are not independent criminal cells — they are coordinated nodes in a single command architecture.
- The anticipated mechanism is simultaneous activation of the 2 lakh staged accounts for high-value transfers, combined with AI-driven digital arrest operations targeting company principals using the 80 million biometric records already held on Chinese servers, and simultaneous UPI/payment gateway manipulation — designed to overwhelm law enforcement response capacity.
- The September/October 2026 timing corresponds to major Indian financial events and the festival season payment volume period (Navratri, Diwali), when transaction scrutiny is reduced by volume and institutional vigilance is typically lower.

I have submitted detailed account-level intelligence on four specific staged accounts to MeitY. I hold approximately 6,000 pages of documented evidence on this ecosystem. I am available to present this evidence in full to the National Security Advisor, the National Cyber Security Coordinator, or any authority designated by the Law Officers, at any time.

6. I write to both the Attorney General and the Solicitor General for a specific reason. You are the Law Officers of the Union. You represent the Government of India before the Supreme Court of India. When the Hon'ble Court resumes after the summer vacation and this matter comes up — whether through a contempt petition or fresh proceedings — you will be the officers standing for the Union. I do not want that to be the first moment at which the Government's most senior law officers are informed of what I have placed before MeitY and this nation.

The Supreme Court has already spoken. A three-judge bench led by the Chief Justice has directed MeitY to act. I am giving the Government six weeks from 19 May 2026 — until approximately **30 June 2026** — to demonstrate a substantive response to the petition. If MeitY fails to respond in a time-bound and substantive manner within that window, I will **move for contempt of court proceedings** before the Supreme Court upon resumption of court after the vacation period.

I respectfully submit that it would be in the interest of the Government, the Court, and most importantly the nation, if the Law Officers were to proactively engage with MeitY, I4C/MHA, and the National Cyber Security Coordinator on the contents of this petition and the anticipatory intelligence submitted herein — before the contempt proceedings become necessary and before the September–October 2026 threat window arrives.

7. I wish to be unambiguous about the nature of this communication. This is not a threat. This is not adversarial. I am not on social media. I have not sought personal recognition for any of this work. I have come to MeitY, I4C, RBI, PMO, and NCSC over five years. I went to the Supreme Court because I had no other door. The Court has now pointed me back to the executive. I am following that direction precisely. I am informing the Law Officers because I believe — without any partisan consideration — that when there are **limited days left to prevent an irreversible harm to this nation**, every constitutional officer must be on notice. I am sending copies of this communication and the attached submissions to the Prime Minister's Office and the National Security Advisor by Speed Post. I am also informing the Treasury and the principal opposition party, as this is a matter that transcends all politics — the nation comes before any government.

8. I respectfully request the following from both the Attorney General and the Solicitor General:

- Kindly take note of the Supreme Court's direction in W.P.(Crl.) No. 163/2026 dated 19 May 2026 and ensure the Government is fully briefed on the contents of the supplementary representation submitted to MeitY.
- Kindly engage proactively with MeitY, I4C/MHA, and the National Cyber Security Coordinator regarding the anticipatory intelligence submission on the September–October 2026 threat window, so that preventive action is taken before the execution window opens.
- Kindly advise the Government to constitute the Data Protection Board under DPDPA 2023 and operationalise the Act without further delay — the statutory framework that could have prevented this ecosystem exists but has not been activated.
- If the Law Officers require a full technical briefing on the 6,000 pages of evidence and the intelligence submissions, I am available in person at any time convenient to both offices.

I close with one submission. A nation's security is not the property of any party, any government, or any institution. It belongs to its citizens. I am one citizen who has spent five years documenting an attack on 80 million of his fellow citizens and who now stands, pursuant to the Supreme Court's own direction, at the door of the executive. The Hon'ble Court has said they shall consider it. I am trusting that they will. And I am trusting that the Law Officers of this Union will ensure that trust is not misplaced.

Nitish Kumar

AI SCHOLAR | DATA SCIENTIST|NATIONAL CYBER SECURITY SCHOLAR -NSD

email: nitish.kumar40@outlook.com |**Mobile:**9082843142

Avoid Corruption! Avoid Racism

supplementaryrepresentationpursuanttothedirectionofth.zip
11907K