

Headlines

Colombo Security Conclave - Page No.6 , GS 2

Speed bumps ahead - Page No.6 , GS 3

Mandating the Sanchar Saathi - Page No.6 , GS 2

Privacy - Page No.7 , GS 2

PM Internship Scheme - Page No.11 , GS 2

Jal Jeevan Mission - Page No.11 , GS 2

Masala Bond – Prelims Fact

“
Life shrinks or
expands in
proportion to
one's courage.

VEDANTA

COACHING ACADEMY & LIBRARY

Anais Nin

Only 20% of candidates accepted PM Internship Scheme offers: data

Page No. 11, GS 2

T.C.A. Sharad Raghavan
NEW DELHI

While the PM Internship Scheme's pilot project has exceeded its target of providing 1.25 lakh internship opportunities in a year, it has found few takers among India's youth, data presented to Parliament show.

Over two phases, 1.65 lakh internship offers were made by companies to applicants, Minister of State for Corporate Affairs Harsh Malhotra informed the Lok Sabha in a reply to a question. Of these offers, only 20% were accepted. Candidates cited locations, roles, and duration as reasons for declining offers. Of those who accepted offers, one-fifth of participants left their internships before completing them.

The Prime Minister Internship Scheme (PMIS) was announced in the Union Budget 2024 with the aim of providing internship opportunities to one crore youth in India's top



Few takers: The Centre says 1.65 lakh internship offers were made by companies to applicants. V. RAJU

500 companies in five years. In October 2024, the Ministry of Corporate Affairs launched a pilot project for the scheme, targeting 1.25 lakh internship opportunities in a year.

Low acceptance rates

Under the first round of the pilot project, companies posted more than 1.27 lakh internship opportunities on the scheme portal, for which 6.21 lakh applications were received. The

companies made 82,000 internship offers, of which 8,700 or 10.6% of the offers were accepted.

The Minister's reply noted that, as of November 26, 4,565 candidates from the first round had left their internships without completing them. That is, more than half the candidates that started their internships in the first round left before finishing their term.

In the second round of the pilot scheme from Ja-

nuary onwards, companies posted over 1.18 lakh internship opportunities for which they received over 4.55 lakh applications. As of November 26, companies have made over 83,000 offers, of which 24,600 offers or 30% were accepted.

So far, 2,053 candidates – or 8.3% of the ones who accepted internships in the second round – have left without completing their internships, the government said.

Taken together, this means that over the two rounds, 1.65 lakh internship offers were made, of which 33,300 (20.2%) offers were accepted. Of those that were accepted, 6,618 (19.9%) candidates quit their internships prematurely.

The government had initially budgeted ₹840 crore for the pilot project, which was revised down to ₹380 crore in the financial year 2024-25. Of this, the pilot project has so far utilised ₹73.72 crore, the reply said.

- While the PM Internship Scheme's pilot project has exceeded its target of providing 1.25 lakh internship opportunities in a year, it has found few takers among India's youth, data presented to Parliament show.
- Over two phases, 1.65 lakh internship offers were made by companies to applicants, Minister of State for Corporate Affairs Harsh Malhotra informed the Lok Sabha in a reply to a question. Of these offers, only 20% were accepted.
- Candidates cited locations, roles, and duration as reasons for declining offers. Of those who accepted offers, one-fifth of participants left their internships before completing them.
- The Prime Minister Internship Scheme (PMIS) was announced in the Union Budget 2024 with the aim of providing internship opportunities to one crore youth in India's top 500 companies in five years.
- In October 2024, the Ministry of Corporate Affairs launched a pilot project for the scheme, targeting 1.25 lakh internship opportunities in a year.

Content.

- Under the first round of the pilot project, companies posted more than 1.27 lakh internship opportunities on the scheme portal, for which 6.21 lakh applications were received. The companies made 82,000 internship offers, of which 8,700 or 10.6% of the offers were accepted.
- The Minister's reply noted that, as of November 26, 4,565 candidates from the first round had left their internships without completing them. That is, more than half the candidates that started their internships in the first round left before finishing their term.
- In the second round of the pilot scheme from January onwards, companies posted over 1.18 lakh internship opportunities for which they received over 4.55 lakh applications. As of November 26, companies have made over 83,000 offers, of which 24,600 offers or 30% were accepted.

Content.

- The scheme aims to provide students with internship opportunities to address youth unemployment.
- It seeks to provide internships to 1 crore young people over the next five years.
- Applicants will get a monthly stipend of ₹4,500 from the government, and an additional ₹500 by companies as part of their Corporate Social Responsibility initiatives consisting of one year.
- A one-time grant of ₹6,000 will be provided upon enrollment, along with insurance coverage under the PM Jeevan Jyoti Bima Yojana and PM Suraksha Bima Yojana.
- Age: 21- 24 years.
- Education: At least Class 10th; graduates from premier institutions (IITs, IIMs) and professional qualifications (CA) are excluded.
- Employment Status: Must not be in full-time employment.
- Income Restriction: Family income must not exceed ₹8 lakh annually; families with government employees are ineligible.

- The term "Corporate Social Responsibility" in general can be referred to as a corporate initiative to assess and take responsibility for the company's effects on the environment and impact on social welfare.
- In India, the concept of CSR is governed by clause 135 of the Companies Act, 2013.
- India is the first country in the world to mandate CSR spending along with a framework to identify potential CSR activities.
- The CSR provisions within the Act is applicable to companies with an annual turnover of 1,000 crore and more, or a net worth of Rs. 500 crore and more, or a net profit of Rs. 5 crore and more.
- The Act requires companies to set up a CSR committee which shall recommend a Corporate Social Responsibility Policy to the Board of Directors and also monitor the same from time to time.
- The Act encourages companies to spend 2% of their average net profit in the previous three years on CSR activities.

Mains Question

- **Q.** *India's demographic advantage risks turning into a liability as skill gaps widen across sectors, even as unemployment persists despite economic growth. Analyse the structural factors driving the skill-jobs mismatch, and suggest measures to align education, skilling, and labour-market needs for inclusive and sustainable employment generation.*
- भारत की जनसांख्यिकीय बढ़त कौशल-अंतराल (Skill Gap) और लगातार बनी बेरोज़गारी के कारण एक संभावित बोझ में बदलती जा रही है। कौशल-नौकरी असंतुलन के पीछे निहित संरचनात्मक कारणों का विश्लेषण कीजिए तथा शिक्षा, कौशल विकास और श्रम बाज़ार की आवश्यकताओं को बेहतर ढंग से जोड़ने हेतु आवश्यक नीतिगत उपाय सुझाइए।

Centre says U.P. reported maximum complaints over Jal Jeevan Mission projects

Page No. 11, GS 2

Jacob Koshy
NEW DELHI

Nearly 17,036 complaints have been received by States and Union Territories on “irregularities” and “poor work quality” in projects initiated under the Jal Jeevan Mission, with about 84% of the complaints coming from Uttar Pradesh.

Action had been taken against 621 Departmental Officials, 969 contractors, and 153 Third Party Inspection Agencies, the Minister of State for Jal Shakti, V. Somantha, said in response to a query in the Rajya Sabha.

The total number of complaints was based on reports tabulated by 32 States and Union Territories, and included a range of sources, including “... media reports, *suo-moto* cognisance, references from public representatives, citizens, and grievance portals”, he said.



Water woes: States and Union Territories reported 17,036 complaints over ‘shoddy’ Jal Jeevan Mission work. FILE PHOTO

Uttar Pradesh reported the highest number of complaints and constituted about 84% of the total complaints received over financial irregularities and poor quality of work under the mission.

Inquiries initiated

“The State reported that it had initiated enquiries in all 14,264 complaints received from various channels, including *suo moto* cognisance, and reports have been submitted in

14,212 cases, while enquiries are under process in 52 cases. The State has further reported that action was taken in 434 cases which involved 171 department level officials, 120 contractors and 143 TPIAs, while the remaining complaints have either been addressed or found irrelevant,” the Minister noted.

After Uttar Pradesh, the States with the most number of complaints are Assam (1,236) and Tripura (376).

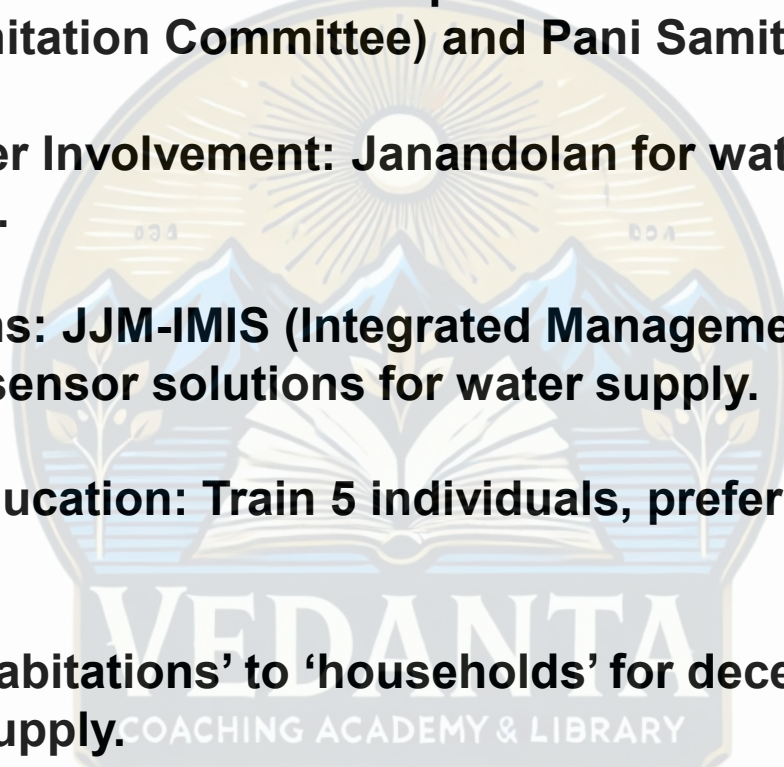
Content.

- **Nearly 17,036 complaints have been received by States and Union Territories on “irregularities” and “poor work quality” in projects initiated under the Jal Jeevan Mission, with about 84% of the complaints coming from Uttar Pradesh.**
- **Action had been taken against 621 Departmental Officials, 969 contractors, and 153 Third Party Inspection Agencies, the Minister of State for Jal Shakti, V. Somanna, said in response to a query in the Rajya Sabha.**
- **The total number of complaints was based on reports tabulated by 32 States and Union Territories, and included a range of sources, including “... media reports, suo-moto cognisance, references from public representatives, citizens, and grievance portals”, he said.**
- **Uttar Pradesh reported the highest number of complaints and constituted about 84% of the total complaints received over financial irregularities and poor quality of work under the mission.**

Fact

- **Launched on 15th August 2019, the Jal Jeevan Mission (JJM) aims to provide tap water to every rural household by 2024 (extended till 2028), targeting 55 liters per person per day. It is a Centrally Sponsored Scheme, implemented by the Ministry of Jal Shakti.**
- **Mnemonic: TAP**
- **T – Target Every Rural Household: Provide Functional Household Tap Connections (FHTC) to all rural households.**
- **A – Areas of Priority: Focus on quality-affected, drought-prone, desert regions, and Sansad Adarsh Gram Yojana (SAGY) villages.**
- **P – Public Places: Ensure taps in schools, Anganwadi centers, gram panchayats, and community buildings.**

- **Mnemonic: WATER**
- **W- Women and Weaker Sections: Ensure 50% representation of women in committees like VWSC (Village Water And Sanitation Committee) and Pani Samitis.**
- **A- Awareness and Stakeholder Involvement: Janandolan for water, encouraging voluntary contributions like shramdaan.**
- **T - Technological Interventions: JJM-IMIS (Integrated Management Information System), real-time Dashboards, IoT-based sensor solutions for water supply.**
- **E - Empowerment through Education: Train 5 individuals, preferably women, per village on water quality testing.**
- **R - Rural Focus: Shift from 'habitations' to 'households' for decentralized, demand-driven, community-managed water supply.**



Mains Question

- Contaminated drinking water has emerged as a major public health and development challenge in India. In this context, evaluate the objectives and implementation effectiveness of the Jal Jeevan Mission, and suggest measures to ensure safe, sustainable, and equitable access to potable water in both rural and urban areas.
- देश में पेयजल प्रदूषण की बढ़ती समस्या स्वास्थ्य, विकास और सामाजिक न्याय—सभी के लिए गंभीर चुनौती बन गई है। इस संदर्भ में, जल जीवन मिशन के उद्देश्यों और कार्यान्वयन की प्रभावशीलता का मूल्यांकन कीजिए तथा ग्रामीण और शहरी क्षेत्रों में सुरक्षित एवं सतत पेयजल उपलब्ध कराने के लिए आवश्यक सुधारात्मक कदम सुझाए।

A template for security cooperation in the Indian Ocean

Page No. 6, GS 2

On November 20, 2025, India hosted the 7th National Security Advisor-level summit of the Colombo Security Conclave (CSC). India's National Security Adviser, Ajit Doval, hosted his counterparts from other member-countries, Sri Lanka, the Maldives, Mauritius and Bangladesh, while counterparts from Seychelles and Malaysia were observer state and guest, respectively. The CSC has sought to position itself as a critical forum to promote and foster cooperation in the domain of security in the Indian Ocean region.

Initiated as a trilateral grouping between India, Sri Lanka and Maldives in 2011, the group lost steam in light of the political transition in the Maldives and Sri Lanka, and lack of convergence among the member-states to identify priorities in security cooperation in the Indian Ocean. The group reconvened its engagement under the aegis of the CSC in 2020, a proposed framework to further cooperation in maritime security, counter-terrorism, trafficking and organised crime and cybersecurity. Since then, the group has remained steady in not just maintaining momentum among its member-states but also inducting countries. In 2022, Mauritius joined as a full member, while in 2024, the group saw the admission of Bangladesh.

A region witnessing shifts

For India, the summit, in 2025, comes at a pivotal moment. Frameworks of cooperation in the maritime domain, in the broader Indo-Pacific, and indeed in the Indian Ocean appear to be undergoing a crucial shift. Given the focus of the CSC on non-traditional issues of maritime security, it is vital to bolster cooperation in mitigating the looming challenges. While the



Harsh V. Pant

is Vice-President,
The Observer
Research Foundation



Sayatan Halder

is Associate Fellow,
Maritime Studies,
The Observer
Research Foundation

There are encouraging signs that member-country engagement is deepening in the Colombo Security Conclave, but challenges remain

Indian Ocean maritime security architecture remains fragmented due to the lack of any singular institutional framework, groups such as the CSC must remain committed to enhancing cooperation in this regard.

The issue of development

Importantly, for the wider Indian Ocean littoral world, and especially the members of the CSC, maritime security challenges are often coupled with their developmental priorities.

Given the extent of dependency these countries have on the oceans for their economic progress, securing challenges emanating from the maritime domain is crucial. In many ways, maritime security challenges are deeply intertwined with the lives and livelihoods of not just the littoral communities in these countries but also appear to unlock new opportunities for their national economies in today's era of sea-borne globalisation.

This year's summit has been crucial in many ways. First, the group saw further expansion by way of accession of Seychelles as a full-member into the forum. This signals a deep commitment among countries in the region to harness cooperation within the mandate of the CSC. Second, for India, the CSC also marks a new step in further deepening engagement with its maritime neighbours, amidst an increasingly volatile geopolitical and security shift that appears to be underway in the region in lieu of China's growing presence and influence.

Third, the summit further underscores the growing vitality of the security dimension in enhancing cooperation to boost regional cooperation in the Indian Ocean.

Fourth, the inclusion of Malaysia in this year's

summit as a guest participant may pave the way for further expansion of the group.

Viewing the China factor

However, as the CSC envisages its expansion and broadening the contours of its agenda, some key challenges appear to be looming. First, for India, a key maritime security priority is anchored in the nature and extent of the Chinese presence in the Indian Ocean. On the other hand, the other member countries of the CSC appear to not view the Chinese presence in the Indian Ocean as a major security challenge given their dependence on Beijing as a key developmental partner. Therefore, a careful balance needs to be achieved by India to address the question of growing Chinese presence in the Indian Ocean.

Second, the CSC must direct efforts to strengthen an institutional framework. At present, the group operates at a National Security Adviser-level structure. With growing synergies among its member-countries, the group must seek to institutionalise cooperation such that it remains consistent in aligning policies with actionable pathways of cooperation.

Third, domestic uncertainties in countries such as Bangladesh, and the ensuing impact on how Dhaka continues to engage with India and the other member-countries may run the risk of uncertainty over the group's resilience.

Given this context, the CSC has made significant advances in heralding a new framework of cooperation in a region that suffers from a deep lack of cohesion and convergence among countries on issues of security. Efforts to imagine the way ahead must remain anchored in the need to foster institutional resilience and cohesion among its member-countries.

Content.

- On November 20, 2025, India hosted the 7th National Security Advisor-level summit of the Colombo Security Conclave (CSC). India's National Security Adviser, Ajit Doval, hosted his counterparts from other member-countries, Sri Lanka, the Maldives, Mauritius and Bangladesh, while counterparts from Seychelles and Malaysia were observer state and guest, respectively.
- The CSC has sought to position itself as a critical forum to promote and foster cooperation in the domain of security in the Indian Ocean region.
- Initiated as a trilateral grouping between India, Sri Lanka and Maldives in 2011, the group lost steam in light of the political transition in the Maldives and Sri Lanka, and lack of convergence among the member-states to identify priorities in security cooperation in the Indian Ocean.

Content.

- The group reconvened its engagement under the aegis of the CSC in 2020, a proposed framework to further cooperation in maritime security, counter-terrorism, trafficking and organised crime and cybersecurity.
- Since then, the group has remained steady in not just maintaining momentum among its member-states but also inducting countries.
- In 2022, Mauritius joined as a full member, while in 2024, the group saw the admission of Bangladesh.
- For India, the summit, in 2025, comes at a pivotal moment. Frameworks of cooperation in the maritime domain, in the broader Indo-Pacific, and indeed in the Indian Ocean appear to be undergoing a crucial shift.

- **Origin and Evolution:** It began in 2011 as the Trilateral Maritime Security Cooperation between India, Maldives, and Sri Lanka.
- **Activity stalled after 2014** due to India–Maldives tensions and shifting geopolitical dynamics.
- **Revived and rebranded as the CSC in 2020.** Membership expanded with Mauritius (2022), Bangladesh (2024) and Seychelles (2025).
- **Objective:** Promote regional security by addressing transnational threats and challenges of common concern to the Member States.

Pillars of Cooperation:

- **Maritime safety and security**
- **Countering terrorism and radicalisation**
- **Combating trafficking and transnational organised crime**
- **Cyber security and protection of critical infrastructure**
- **Humanitarian assistance and disaster relief (HADR)**



Speed bumps ahead

The third quarter is unlikely to bring cheer for the economy

The last few days have shown just what a roller coaster of a ride India's economic data can take. Last Friday's robust Q2 GDP growth, a six-quarter high of 8.2%, lifted the government's mood and brought cheer to its supporters. The relatively low nominal growth rate and grade by the IMF did little to dampen this feeling. However, the latest data on the Index of Industrial Production (IIP) and, to an extent, the manufacturing PMI are likely to do more in that regard. The IIP's growth in October 2025 was just 0.4%, a 14-month low. While the GDP data for the July-September quarter showed the manufacturing sector growing 9.1%, the IIP showed the sector had slowed to a 14-month low of 1.8% in October. One of the possible reasons for this is that the GDP growth rate was boosted by a low base, since the sector had grown just 2.2% in the July-September 2024 quarter. The other, more troubling reason, is the impact of the U.S.'s tariffs. Merchandise exports grew in September, the first full month of 50% tariffs, as earlier orders were being fulfilled. They then contracted nearly 12% in October as the tariffs began to weigh on new order decisions. The PMI data, too, showed that the score for India's manufacturing sector stood at a nine-month low of 56.6 in November. The report specifically mentioned that new export orders rose at their slowest pace in over a year, another sign that the U.S.'s tariffs were hurting.

While subdued exports likely weighed on the manufacturing sector, the change in weather towards winter and prolonged rains pulled down the electricity and mining sectors, respectively. As a result, the primary goods sector contracted in October. The GDP data had shown that investment had grown by a reasonably strong 7.3% in Q2. However, the IIP data suggest this could have slowed in the beginning of Q3 with the capital goods sector growing at a 14-month low of 2.4%. The IIP data also have some concerning news regarding household consumption. The GDP data showed that Private Final Consumption Expenditure grew at nearly 8% in Q2. However, the IIP showed that the consumer durables and non-durables sectors contracted in October, in aggregate their worst performance in two years. This was the first full month of data following the GST rate rationalisation. GST revenue of ₹1.7 lakh crore in November, reflecting economic activity in October, also shows that demand did not come rushing in as fast as the government would have liked. Taken together, multiple initial metrics are indicating that Q3 is not likely to be a cheerful quarter for the economy.

Page No. 6, GS 3

Content.

- **The third quarter is unlikely to bring cheer for the economy**
- **While subdued exports likely weighed on the manufacturing sector, the change in weather towards winter and prolonged rains pulled down the electricity and mining sectors, respectively. As a result, the primary goods sector contracted in October.**
- **the IIP showed that the consumer durables and non-durables sectors contracted in October, in aggregate their worst performance in two years. This was the first full month of data following the GST rate rationalisation.**
- **GST revenue of ₹1.7 lakh crore in November, reflecting economic activity in October, also shows that demand did not come rushing in as fast as the government would have liked. Taken together, multiple initial metrics are indicating that Q3 is not likely to be a cheerful quarter for the economy.**

Zero stars

Mandating the Sanchar Saathi app to tackle cybercrime is an overkill

The growing sophistication of cybercrimes, from “digital arrests” to anonymous, large-scale cross-border scams, has made tackling them both urgent and difficult. Cybercriminals have exploited a security gap wherein user accounts on instant messaging apps remain functional even after the associated SIM card has been removed, using this anonymity to conduct government impersonation fraud. The rampant use of spoofed or tampered IMEI numbers has also made tracking perpetrators nearly impossible for law enforcement. It is perhaps inevitable that the government seeks sharper tools to address these software and hardware vulnerabilities, which explains the Department of Telecommunications’ directives on November 28 and December 1. The first mandates “SIM binding” – ensuring that a user’s account is disabled if the physical SIM is removed. In the second, smartphone manufacturers must pre-install the Sanchar Saathi app to verify device authenticity in all new devices by March 2026. While the first directive is a security patch which could inconvenience WhatsApp/Internet messaging users, the second is reminiscent of the saying, the road to hell is often paved with good intentions. The solution to the problem of counterfeit handsets and spoofed IMEI numbers is a cure that could potentially be more damaging than the disease.

The explicit instruction in the directive that the app is “readily visible and accessible to the end users at the time of first use or device setup and that its functionalities are not disabled or restricted” would mean that this app will be given a higher security clearance within the phone’s operating system, allowing it more intrusive access to features such as camera, phone or SMS access. The potential for misuse of this app for state surveillance and being utilised by a malicious entity after compromise to target millions of users is very present and clear. This is no empty fear considering what the Union government has done with the use of Pegasus software to target the political opposition, journalists and activists. Notwithstanding Union Minister Jyotiraditya Scindia’s clarification that users could delete the app, the directive’s text mandating that it cannot be disabled suggests that it will function more as a Panopticon and less as a simple verification tool. As the Supreme Court’s K.S. Puttaswamy (2017) judgment established, any state intrusion into privacy must satisfy the tests of legality, necessity, and proportionality. The government already possesses less intrusive means to verify device genuineness. The Sanchar Saathi web portals, SMS-based checks, and USSD codes should suffice. By ignoring these less invasive alternatives, the directive on Sanchar Saathi fails the proportionality standard. It is little wonder that privacy-conscious manufacturers such as Apple have reportedly refused to comply with this order.

Page No. 6, GS 2

Content.

- The growing sophistication of cybercrimes, from “digital arrests” to anonymous, large-scale cross-border scams, has made tackling them both urgent and difficult.
- Cybercriminals have exploited a security gap wherein user accounts on instant messaging apps remain functional even after the associated SIM card has been removed, using this anonymity to conduct government impersonation fraud.
- The rampant use of spoofed or tampered IMEI numbers has also made tracking perpetrators nearly impossible for law enforcement.
- The first mandates “SIM binding” — ensuring that a user’s account is disabled if the physical SIM is removed. In the second, smartphone manufacturers must pre-install the Sanchar Saathi app to verify device authenticity in all new devices by March 2026.
- While the first directive is a security patch which could inconvenience WhatsApp/Internet messaging users, the second is reminiscent of the saying, the road to hell is often paved with good intentions.

Privacy in a 'fishbowl society'

In the age of Artificial Intelligence (AI), technology is a double-edged sword, with users grappling with the trade-offs between convenience and privacy. While India has a normative privacy framework in terms of the *Puttaswamy* judgment (2017); the Information Technology Act, 2000 and its Intermediary Guidelines; and the Digital Personal Data Protection Act, 2023, and Rules, the reality of privacy remains opaque.

We now live in a fishbowl society where we are gauging 'harm' from a myopic lens of privacy and dignity instead of obscurity. As Meredith Broussard notes in her book *Artificial Unintelligence*, society's over-reliance on technology is leaving us ill-prepared to cope with the very systems we have built. This not only exposes individuals to the risks of data breach but also pushes them into obscurity, especially in cases of Non-Consensual Intimate Image Abuse (NCII), where algorithms generate deepfake pornographic images without one's knowledge or control. Regulating such an assault is an urgent legal and policy imperative. The conventional frameworks for addressing such abuses are inadequate. Traditional approaches often describe risks of any such surveillance as loss of privacy, when in reality it is many more things as well: anxiety, chronic fear of being watched, victim blaming and shaming, societal stigma, career stagnation, permanent loss of autonomy, and bodily integrity.

Laws are not enough

Surprisingly, despite cybercrimes being on the rise, there is no contemporary data on NCII. Data of the National Crime Records Bureau (NCRB) puts all cybercrimes in one category, without any granular classification of specific offences. We filed an Right to Information application on October 3, 2025 seeking



Aastha Tiwari

Assistant Professor (Law) and PhD scholar, Maharashtra National Law University Mumbai



Shweta Bhuyan

Research Assistant (Law) and PhD scholar, Maharashtra National Law University Mumbai

The government has issued Standard Operating Procedures to curb the circulation of Non-Consensual Intimate Image Abuse. But this is only a starting point

information on the number of cases registered in the previous year relating specifically to cyberbullying and cybervoyeurism, along with the gender-wise distribution of victims. After more than a month, the Ministry responded that "law and order" and "police" fall under the State List, and therefore, the most appropriate authority to furnish such information would be the respective State governments.

This shows that mere legal provisions are not sufficient to address the realities of online abuse. Accessibility, awareness, and social acceptance of these laws play an equally critical role in determining their effectiveness. A significant share of young women are unaware of what offences such as voyeurism or deepfake porn legally entail. The lack of digital literacy is compounded by deep-rooted social stigma, shame, and fear of blame, which often deter victims from reporting. In extreme cases, this has driven some survivors to self-harm.

Going beyond an SOP

On November 11, 2025, the Ministry of Electronics and Information Technology issued Standard Operating Procedures (SOPs) to curb the circulation of NCII. These guidelines mandate that such content must be taken down within 24 hours of reporting and seek to safeguard the "digital dignity" and privacy of women by offering multiple platforms for complaints. This is a welcome and long-awaited step. However, an SOP is only the starting point. Its effectiveness depends on being backed by strong capacity-building programmes, stakeholder consultations, and strengthening of enforcement agencies.

A key limitation lies in the absence of a gender-neutral framework. Studies show that transgender persons, particularly transwomen, are disproportionately targeted through deepfake-based harassment. Yet the SOP is silent on transgender victims,

overlooking the Supreme Court's recognition of transgender persons as the "third gender" entitled to equal rights. Further, it does not establish clear accountability mechanisms, define the quantum of punishment, or articulate specific regulations for deepfake generation, dissemination, and tracing. Thus, having a dedicated law on NCII is the need of the hour – one that goes beyond the traditional focus on *actus reus* and *mens rea* and emphasises explicit duties on platforms, AI developers, and intermediaries, more specific and comprehensive than the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rule, 2025.

With the proliferation of AI-generated deepfakes, mainly used to harass, shame, and silence victims (mostly women), privacy is increasingly shaped and threatened by technological capabilities rather than legal protections. The lack of procedural safeguards, traceability norms, and independent oversight mechanisms has allowed such crimes to go unreported and unpunished for years, even as their frequency and severity escalate. These challenges raise an important question: Is an SOP enough?

Lack of awareness of rights or even of what "voyeurism" or "revenge porn" legally constitutes, inadequate sensitisation of police officials, victim-blaming, and deficient cyber-investigative capacity further dilute the impact of existing laws. As NGOs and research studies highlight, thousands of cases are filed daily across India, yet convictions remain disproportionately low. In this context, while the SOP is a crucial first step, a meaningful response to NCII and deepfake harms requires gender-neutral reforms, police training, capacity building, platform accountability, AI-specific safeguards, and stronger victim-centric legal mechanisms.

Content.

- In the age of Artificial Intelligence (AI), technology is a double-edged sword, with users grappling with the trade-offs between convenience and privacy.
- While India has a normative privacy framework in terms of the Puttaswamy judgment (2017); the Information Technology Act, 2000 and its Intermediary Guidelines; and the Digital Personal Data Protection Act, 2023, and Rules, the reality of privacy remains opaque.
- As Meredith Broussard notes in her book Artificial Unintelligence, society's over-reliance on technology is leaving us ill-prepared to cope with the very systems we have built.
- This not only exposes individuals to the risks of data breach but also pushes them into obscurity, especially in cases of Non-Consensual Intimate Image Abuse (NCII), where algorithms generate deepfake pornographic images without one's knowledge or control.

Fact

- **Regulating such an assault is an urgent legal and policy imperative. The conventional frameworks for addressing such abuses are inadequate.**
- **Traditional approaches often describe risks of any such surveillance as loss of privacy, when in reality it is many more things as well: anxiety, chronic fear of being watched, victim blaming and shaming, societal stigma, career stagnation, permanent loss of autonomy, and bodily integrity.**
- **Surprisingly, despite cybercrimes being on the rise, there is no contemporary data on NCII. Data of the National Crime Records Bureau (NCRB) puts all cybercrimes in one category, without any granular classification of specific offences.**
- **“police” fall under the State List**

Fact

- **With the proliferation of AI-generated deepfakes, mainly used to harass, shame, and silence victims (mostly women), privacy is increasingly shaped and threatened by technological capabilities rather than legal protections.**
- **The lack of procedural safeguards, traceability norms, and independent oversight mechanisms has allowed such crimes to go unreported and unpunished for years, even as their frequency and severity escalate.**
- **Lack of awareness of rights or even of what “voyeurism” or “revenge porn” legally constitutes, inadequate sensitisation of police officials, victim-blaming, and deficient cyber-investigative capacity further dilute the impact of existing laws.**
- **Voyeurism is the sexual interest in or practice of watching other people engaged in intimate behaviors, such as undressing, sexual activity, or other actions .**

Masala Bond

Masala Bonds

**A rupee denominated bond issued overseas by
an Indian entity**



Content.

- **Masala Bonds are rupee-denominated bonds issued overseas by Indian entities to raise funds, where the currency risk is borne by the investor, not the issuer.**
- **Introduced in: First issued globally by IFC in 2014 (₹1,000 crore) and officially allowed by RBI in 2015 under its rupee-denominated bond framework.**

Objective:

- **To allow Indian corporates, NBFCs and infrastructure trusts to raise global capital in rupees.**
- **To reduce reliance on Foreign Currency borrowings (ECBs) and shift exchange rate risk to investors.**
- **To deepen offshore rupee markets and promote internationalisation of the Indian rupee.**

Historical Context:

- **Rupee-denominated:** Bonds priced in INR but subscribed overseas; redemption also paid in INR.
- **Eligible issuers:** Indian corporates, NBFCs, REITs, InvITs.
- **Listing:** Can be listed on global exchanges (e.g., London, Singapore).
- **Minimum maturity:** Initially 5 years, later reduced to 3 years.
- **Reduced currency risk** for Indian issuers and improved cost of borrowing versus domestic bonds.



Who Can Invest?

- **Investors outside India who would like to invest in assets in India can subscribe to these bonds. Any resident of that country can subscribe to these bonds which are members of the Financial Action Task Force (FATF).**
- **That includes individuals, institutions, and even financial organisations from countries that follow international standards for fair and secure investing, like those under IOSCO (International Organisation of Securities Commissions).**
- **It also covers multilateral and regional financial institutions of which India is a member.**

Thank You!

