DAILY CURRENT AFFAIRS

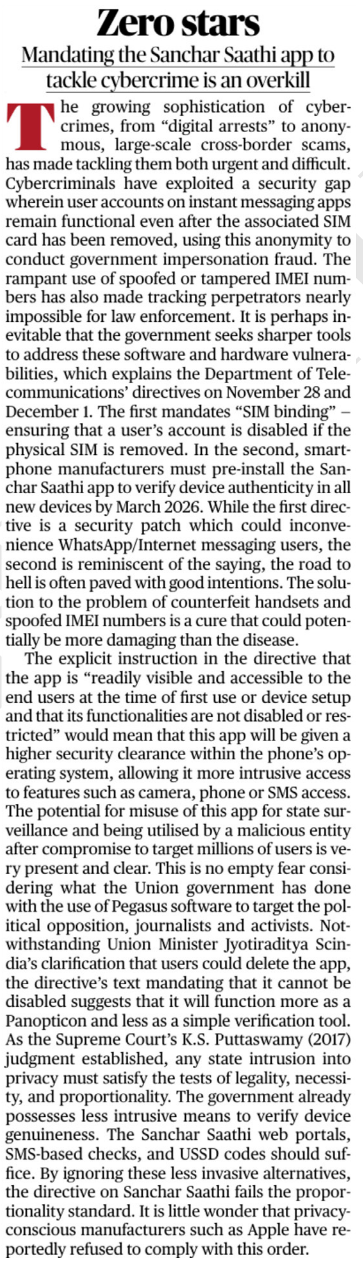
3rdDecember, 2025

The Hindu Analysis 3rd December 2025

Topics Covered

- Sanchaar Saathi App, Pg-6
- A template for security cooperation in the Indian ocean, Pg-6
- Privacy in a fishbowl society, Pg-7
- Jal Jeevan Mission , Pg-15
- PM Internship Scheme, Pg-15

Page-6



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.

A template for security cooperation in the Indian Ocean

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 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.

Harsh V. Pant

is Vice-President, The Observer Research Foundation

Sayatan Haldar

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

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.

Page-7

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 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.

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

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.

Page-15

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

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. 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.

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).

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

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 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.

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

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 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.

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.