Text of Keynote address by Sh. Amit Agrawal, Secretary to the Government of India, Department of Telecommunications, at the Thematic Panel Discussion I: Cybersecurity and Trustworthy ICTs, including Child Online Protection

Digital BRICS Forum, Pune

प्रविष्टि तिथि: 20 AUG 2026 9:09PM by PIB Delhi

Distinguished delegates from BRICS member countries, representatives from the Government of India and the Governments of various States of the Union of India, industry and academia, ladies and gentlemen,

I wish you all a good afternoon.

Since inception of the BRICS Information and Communication Technology Track in 2016, the focus has been mostly on the number of people digitally connected and the reach of digital networks. In the decade since, BRICS countries have made significant progress, with digital connectivity in the five founding BRICS member countries growing by 1.3 billion internet users — from about 45% in 2016 to about 82% today — and 4G coverage expanding from about 84% to about 99% of the combined population.

Beyond coverage, BRICS countries have registered their ability to not only secure connectivity for their people but also to contribute to shaping the ongoing digital transformation in terms of digital public infrastructure for delivery at population scale and frontier technologies for transformational gains. This success in expanding digital reach coupled with digital delivery at scale of a growing array of services and

use cases have made it imperative that safety and trust in our ICT systems be recognised and pursued as central to our ICT agenda. And as frontier technologies like AI have made digitalisation more potent, risks have grown alongside gains. Among these risks, effective mitigation of risks to our vulnerable users must assume special attention.

To simultaneously address both digital enablement and safety and trust in digital systems, the two need to be viewed as activities that are not sequential but simultaneous. Safety and trust, and protection of vulnerable users, should be by design and not as an afterthought or reaction. This requires action on three key pillars for securing digital enablement in a safe and trustworthy manner. First, creation of digital public infrastructure that is safe by design. Second, obligations under law for those delivering digital content or collecting digital personal data to do so in a safe and trustworthy manner. Third, empowerment of individuals by law and born-digital mechanisms to secure their rights and effective redress of their grievances.

Let me illustrate each of these three pillars of safe and trustworthy digital enablement from the Indian experience.

The first pillar of safe digital infrastructure by design is exemplified by Aadhaar, India's foundational digital identity and the Unified Public Interface or UPI, its digital public infrastructure for real-time payments. Aadhaar enrolment requires only biometrics, name, gender, date of birth and address and ensures that the biometrics are never shared by the Aadhaar system with those providing digital services and also that the Aadhaar system never has visibility on the details of serviced individuals or their transactions. This separation of identity and service provision ensures safety by design. The trust this has engendered has made Aadhaar near-universal despite enrolment for Aadhaar being voluntary, with 1.4 billion Aadhaar holders performing over 170 billion authentications for purposes ranging from obtaining subsidies and benefits under government programmes and making online payments to fulfilling know-your-customer requirement for opening bank accounts and obtaining mobile sims or establishing identity as a voter. Aadhaar has also enabled a near-universal digital pipeline that connects a billion-plus digital identities with a billion-plus mobile phones and a billion-plus digitally linked bank accounts. Riding on this, UPI has made India home to nearly half of the world's real-time payments each month. And since UPI too minimises by design the sharing of bank details between the transferor and the transferee, despite unmatched scale, the incidence of fraud on UPI is merely 0.02 per million transactions, which is merely 0.2 percent of the 10-per-million fraud incidence rate in the credit and debit card payment system.

The second pillar of obligations under law for those collecting digital personal data or delivering digital content to do so in a safe and trustworthy manner is exemplified by India's future-ready Information Technology Act, 2000 and its Digital Personal Data Protection Act, 2023, which will come into force in May next year. Under the Information Technology Act, safe harbour protection available to intermediaries comes with the obligation to observe due diligence to not allow hosting or sharing of harmful or unlawful content, and to take down such content upon arising of knowledge. Under this, every person has been empowered to directly seek resolution from a social media platform for content that is harmful or invasive of an individual's privacy. In addition, the larger social media intermediaries have the additional obligation to proactively detect harmful or invasive material using automated tools and to publicly self-report the measures taken every month. The impact of this obligation is illustrated by the fact that in a recent month, two of the world's largest social media platforms have reported that they, on their own, have detected and removed close to 875,000 pieces of harmful or invasive material in a single month. Social media platforms have also been obligated to observe due diligence to label Synthetically Generated Information, such as images generated using AI, and to ensure that the label remains intact while sharing. Such safeguards to mitigate harm through use of social media platforms and AI under a law that was enacted even before social media or AI became a reality have proved possible due to India's approach of future-ready,

principle-based lawmaking. The Digital Personal Data Protection Act similarly safeguards children by categorically prohibiting processing of child's data without verifiable parental consent as well as the tracking or behavioural monitoring of children or targeted advertising directed at them.

The third pillar of empowerment of individuals to secure their rights and effective redress of their grievances is exemplified by the born-digital mechanisms provided under these two Acts. If an online grievance relating to violation of digital rights lodged by an affected person is not resolved within tight, specified timeframes, she or he can escalate it with a single click to a Grievance Appellate Committee of independent experts. The committee has served as an effective online mechanism for resolution through disposal of over 10,000 appeals since 2023. The Digital Personal Data Protection Act too provides a similar at-a-click inexpensive and effective digital adjudication mechanism for unresolved grievances through the Data Protection Board of India.

With the BRICS countries accounting for about three-fifths of the world's ICT specialists, about half of its population, about two-fifths of its GDP, the major proportion of digital public infrastructure deployed and two of the top five countries globally in AI inventions, the safety and trust measures BRICS members put in place contribute not only to making their own people more secure but also the world. The strengths, scale and diversity of BRICS countries make them the crucible in which the ICT safety solutions of the world as a whole would be increasingly forged.

I am confident that the deliberations in today's session on Cybersecurity and Trustworthy ICTs, including Child Online Protection would be substantive and help us take this agenda forward.

Thank you.

> Digital BRICS Forum2026
>
> Building a safe and trustworthy digital future through stronger cybersecurity, trusted technologies and resilient digital ecosystems.#DigitalBRICSForum #BRICS2026 #Cybersecurity #TrustworthyICTs #DigitalTrust #BRICSIndia@JM_Scindia @PemmasaniOnX… pic.twitter.com/i0BuXslaZC
>
> — DoT India (@DoT_India) August 20, 2026

***

NJ/ ARJ

(रिलीज़ आईडी: 2301737) आगंतुक पटल : 558
इस विज्ञप्ति को इन भाषाओं में पढ़ें: Urdu , हिन्दी