TRUSTED
INFORMATION
ALLIANCE

TIACON 2025

Information & Trust in the AI Age

Conference Report

Published by
TIA Secretariat
November 2025

BOOM
FACT Crescendo
FACTLY
First Check

INDIA TODAY FACT CHECK
newschecker
NewsMeter
NEWSMOBILE

Tattle
TELUGU POST
the quint
THIP THE HEALTHY INDIAN PROJECT

विश्वास.News

trustedinfoalliance.in
hello@trustedinfoalliance.in

Executive Summary

What does it mean to trust information that is available on digital platforms in the age of AI? This question brought together over 160 participants from across India’s media, technology, policy, civil society, and academic communities at TIACON 2025, a one-day flagship conference hosted by the Trusted Information Alliance (TIA) in New Delhi.

Across five panels, nine project showcases, and one hands-on workshop, attendees explored the real-world implications of AI-generated content, financial scams, and marketplace deception while proposing cross-sectoral approaches that can strengthen trust in digital spaces. The day was not just a dialogue about problems, it was a collective call to design better systems, narratives, and safeguards for the information ecosystem.

At TIA, we no longer define "information" in traditional silos. A six-second reel about an earthquake, a YouTube explainer on personal finance, a 4.5 star product review on a shopping app, or a comment correcting a medical myth on a social media platform—all of these are forms of digital information and they share our perception, choices, and behaviour.

But how much of this information available online can be verified? And what happens when the unverifiable, misleading, manipulated, or malicious information dominates online spaces?

TIACON 2025 tackled these questions head-on, spotlighting urgent themes:

- In healthcare, misinformation is leading to misdiagnosis, broken trust, and poor outcomes. Doctors now compete with social media influencers and AI-generated content for patient trust. As one panelist said, *“If the battle is on Instagram, that’s where we must show up.”*

- In digital marketplaces, the pace of deceptive ads, fake reviews, and dark patterns has outpaced regulation. Platforms and regulators are moving from reactive takedowns to preventive detection systems—training sellers, scanning for fakes, and building media literacy at scale.

- On the domain of AI-generated content, panelists debated whether synthetic media could ever be truly "safe." The legal system is yet to catch up, and watermarking or labeling methods remain fragile. Still, the panel pushed for responsibility-oriented literacy and not just functional awareness.

- In financial fraud: Deepfakes, impersonation, and phishing are now mainstream. A recurring insight throughout the session remained that the burden is falling on victims who must be hyper-vigilant. Scam literacy must become public education and not just private caution.

- In policy: The dilemma persists—can regulation curb misinformation without silencing dissent? Questions around the accountability of government-run fact-check units, content takedown trends, and definitional clarity remain unresolved. The need for checks, transparency, and collaborative frameworks has never been more urgent.

In the ‘Show & Tell’ segment, TIA members presented innovations in: scam detection, AI uses-cases for different journalism functions, media literacy interventions, community engagement models such as trainings using deepfake simulations that teaches people to identify synthetic media and introduced multilingual tools for public education.

At its heart, TIACON 2025 was about convening people who don’t always share the same vocabulary but are united by the same urgency.

Urgency to protect public trust. Urgency to make information work for people, not against them. Urgency to move beyond individual fixes and toward shared stewardship of the digital space.

Unfolding the Health Infodemic:
Providing Accurate and Trusted Health Information for a Healthier India

The inaugural panel ‘Unfolding health infodemic’, featured leading voices from India’s medical and media fraternity who came together to address one of the most pressing challenges in healthcare today—the rampant spread of misinformation and its growing impact on public health and trust in the medical system.

The discussion, moderated by Sudipta Sengupta, CEO-Founder, The Healthy Indian Project (THIP), featured eminent experts, including Dr Heena Tabassum, Senior Scientist and Program Officer, Dept of Non-Communicable Diseases, ICMR; Dr Anand Prakash, Honorary Joint Secretary, Indian Medical Association (IMA); Dr Ashok Mittal, Medical Director and Head – Minimal Access Surgery Department, RG Stone Urology & Laparoscopy Hospital, East of Kailash, and Dr Yugal Karkhur, Senior Consultant, Orthopaedics, Narayana Health.

Here are the key-takeaways from our panel discussion:

On Public Health

True health is a state of complete physical, mental, and social well-being. Misinformation spreads faster because it connects emotionally and is easily accessible on social media.

India’s large population amplifies disease statistics, leading to the global misconception of India as the “diabetes” or “cancer capital.” To project India’s strong national health programs and ongoing public health progress, we need better communication strategies on a national level.

‘Public health’ is about communities rather than individuals. Training local and tribal leaders to communicate accurate health information can help create community-level awareness and a preventive mindset.

Doctor-Patient communication

Communicating with patients has become more challenging for doctors as patients arrive with preconceived notions shaped by online content. This underscores the need for realistic communication and transparency, such as during the first meeting, doctors should be upfront about what is curable and what is not. Communication is not formally taught in medical schools, yet it is as vital as clinical knowledge.

A panelist suggested giving patients verified reading material and using pamphlets to bridge the information gap. "There are two phases to tackling misinformation," the panelist said. "First, you fight it; then, you fact-check it. The government must also sponsor positive and credible information campaigns to ensure truth reaches the public."

Misinformation is not the only challenge

The challenge is not only misinformation but also resistance to understanding. While rural communities are generally receptive and willing to learn, urban populations often dismiss medical advice, relying instead on social media and search engines.

"Many people believe Google cannot be wrong, but a doctor can," a panelist remarked, capturing the growing trust gap between medical professionals and the public.

Digital Engagement

Doctors must be visible where misinformation originates. "If the battle is on Instagram, that's where we must fight it," a panelist said, citing examples of misinformation about vaccines and treatments that have directly harmed patient outcomes, including cases where online myths led people to reject medically advised therapies.

Trust in Doctors

There is also a growing scepticism toward doctors, especially in urban settings, where patients question whether recommendations are motivated by profit. "Once patients start seeing clinicians as service providers rather than healers, both sides lose trust," a panelist cautioned.

As the panel put it succinctly, the path forward lies in "showing up more, showing up differently, and making the truth visible."

Deceptions in the Digital Marketplace: Empowering Indian Consumers To Make Informed Choices Online

The panel discussion on consumer protection was moderated by *The Core*'s Govindraj Ethiraj and featured eminent guests including Saheli Sinha, Director of Operations at the Advertising Standards Council of India (ASCI), Prachi Buchar, Head of Government Relations and Public Policy at Meesho, a content creator on

LinkedIn Jayant Mundhra and Amar Deep Singh, CUTS International, a consumer advocacy and public policy organisation.

Here are the key-takeaways from our panel discussion:

- The era of slow, corrective regulation is over.
- "A TV ad once ran for months. Now one appears and disappears in 24 hours," said a panelist.
- ASCI examined over 6,000 ads this year and nearly 4,500 of them were found to be linked to illegal offshore betting.
- To counter deception, it is focusing on prevention through advertiser training, studying dark patterns like "only four left" scarcity messages and "drip pricing", and developing tools that help brands self-audit before launch
- Fake reviews and counterfeit goods remain persistent risks. Many small sellers, unfamiliar with IP rules, assume what is legal offline works online.
- Meesho, a digital marketplace, now uses optical character recognition to detect fake logos in images and blocks reviews from unverified purchases or identical IP addresses.
- One of the panelists said, "There's an entire industry that writes reviews and it is very lucrative."
- For content creators, the incentives seem to be murkier. Agencies routinely pay influencers to push pre-packaged narratives, often attacking rival platforms or brands.
- "You're handed statistics and told to post. It's quick money, zero verification," explained a panelist.
- The flood of online information has outpaced literacy.
- CUTS International is training 20,000 MSMEs, mostly women-led, in cybersecurity and e-commerce awareness to make both sellers and buyers safer.

AI Content and Reality: Safeguarding Citizens From Harmful and Misleading AI-Generated Content

'AI content and reality', a panel discussion on the harm caused by misleading Ai-generated content was moderated by Tarunima Prabhakar, co-founder of Tattle Civic Technologies, where the panelists examined the existing safeguards and systems that need to be put in place to protect the general public from harm.

The panel featured eminent speakers including Nikhil Naren: Assistant Director, Cyril Shroff Centre for AI, Law and Regulation; Assistant Professor, OP Jindal; Shakoor Rather: Co-founder, Science Matters; Geetha Raju: Senior Policy Analyst on deepfake detection; Sachin Dhawan, The Dialogue.

Here are the key-takeaways from our panel discussion:

A significant challenge lies in the absence of tools capable of demarcating synthetic text. This raises the question: Does the act of labeling content diminish its persuasiveness?

There are inadequacies in the current AI literacy framework, necessitating a shift from functional to responsibility-oriented literacy. Key considerations include:

- **Demographic Inequity**: The role and support for staff within the broader context of AI literacy are often overlooked.

- **Proactive Measures**: A transition from reactive responses to harmful synthetic media towards proactive strategies is crucial for preventing misinformation, as exemplified by the EU Digital Services Act.

- **Core Principles**: Sustainability and climate change must be central tenets of any AI literacy framework.

- **Unequal Value Chain**: An examination of who primarily benefits from the creation of AI value chains is warranted.

The potential for synthetic media to be utilized for beneficial purposes is evident, including:

- **Content Creation and Education:** Enhancing the capabilities of content creators and enriching educational materials.
- **Misinformation and Disinformation:** Conducting thorough risk analyses for synthetic media.
- **Technological Solutions:** Implementing watermarking techniques for identification.

The current legal landscape lacks adequate provisions for redress regarding issues arising from AI.

- **Existing Framework:** The legal system primarily addresses users and platforms responsible for user-generated content.
- **AI's Role:** The emergence of AI introduces new complexities for which the law currently lacks clear rules and guidelines.
- **Regulatory Focus:** The primary regulatory focus remains on platforms and intermediaries.
- **Legal Literacy:** There is a critical need for enhanced legal literacy regarding individual actions, proactive measures by platforms, and interventions by state-instituted legal committees to resolve these issues.
- **Terminology:** The concept of Synthetically Generated Information (SGI) is relevant in this context.

The effectiveness of labeling mechanisms is a subject of debate:

- **Social Labeling:** Socially based labeling may prove ineffective.
- **Technical Labeling:** Technical labeling mechanisms are

susceptible to circumvention.

- **Persistent Relevance:** Despite these challenges, the concept of labeling continues to hold currency.
- **Human Labeling:** Human-based labeling methods are inherently fragile.
- **Cryptic Labeling:** Cryptic labeling offers a more robust implementation strategy.
- **Current System:** The existing system relies on the due diligence of intermediaries.

Scamland-India Fights Back: Helping Digital Nagriks Protect Themselves from Online Scams and Fraud

The Scamland panel, was led by The Quint's fact-checking editor and TIA governing council member Abhilash Mallick, discussed measures that are currently in place to combat this growing menace, what challenges continue to persist, and how we can better safeguard citizens in the digital age.

The panel included ex-DGP Goa Dr Muktesh Chander, cultural heritage technocrat Dr Navina Jafa, senior editor at Jagran New Media Urvashi Kapoor, and the editor of Boom's Decode, Adrija Bose.

Here are the key-takeaways from our panel discussion:

- Digital penetration in rural areas has made it easier for fraudsters to operate. Mobile phones and bank accounts have become convenient tools for committing financial fraud. Among many locals, there appears to be little hesitation or moral conflict around participating in such activities—perhaps because scamming is not perceived as severely as other forms of harm. As a result, it has increasingly become a viable "career option" for some young men.

- Scammers use sophisticated impersonation tactics. Fraudsters often replicate official identities — such as financial regulators or government agencies — using familiar logos, WhatsApp profiles, and APK files to appear legitimate. Victims are frequently placed under psychological pressure, including forms of "digital arrest," and scammers may possess sensitive personal information, such as Aadhaar details.

- Financial losses can be recovered, but only partially and only when acted upon immediately. Rapid reporting through official cybercrime channels significantly increases the chances of recovering funds, although victims often regain only a portion of what is lost.

- Current systems are not fully equipped to handle the human cost of digital fraud. The ease of acquiring SIM cards through

KYC loopholes contributes to the proliferation of scams. With limited traceability of callers and anonymous online communication, users must assume high levels of personal vigilance.

- Deepfake-based fraud is becoming mainstream. Manipulated videos featuring well-known personalities endorsing investment or financial schemes are misleading a wide segment of the population, especially those unfamiliar with digital manipulation.

- Transparency from platforms is critical. Regular transparency reports can meaningfully enhance accountability, offering visibility into the nature and scale of digital fraud and misinformation.

- Scam literacy must become a mainstream public education priority. Content itself is increasingly being weaponised. Cross-sector collaboration among fact-checkers, technologists, cyber experts, and civil society is essential to strengthening digital resilience. Training programmes reveal that scam experiences are far more widespread than publicly acknowledged.

- Digital hygiene practices can significantly reduce vulnerability. Recommended practices include avoiding unsolicited apps or files, maintaining extreme caution with unknown callers, and removing or masking sensitive financial information such as CVV numbers from credit/debit cards.

Is Regulation The Answer: Examining Legal and Policy Frameworks to Tackle Misinformation

The panel titled “Is Regulation the answer? Examining Legal and Policy Frameworks to Tackle Misinformation” was moderated by India Today’s fact-checking editor and TIA governing council member Bala Krishna where they tried to answer the questions —“can regulatory interventions truly curb the misinformation epidemic? And how do we ensure that such measures do not undermine the fundamental right to freedom of speech and expression?”

The panel featured Apar Gupta, the founder-director of the Internet Freedom Foundation, Iyan Karthikeyan, the mission director of the Tamil Nadu government’s Fact-Check Unit, and Rakesh Maheshwari, ex-senior director of Cyber Security and Data Governance at the Ministry of Electronics and Information Technology (MeitY).

Here are the key-takeaways from our panel discussion:

- Defining "misinformation" remains contested. The absence of a universally accepted standard for what constitutes misinformation, especially in the case of state-run units, creates conflict that undermines the work of journalistic fact-checking organisations/teams.

- State-run fact-check units risk blurring the line between verification and censorship. When the authority to label content as "misinformation" rests with the same institutions that are active political actors, it creates a structural conflict of interest. This concentration of power heightens the risk of overreach, particularly during sensitive public events, and raises questions about how to safeguard fact-checking from becoming a tool of narrative control rather than public accountability.

- Content takedown trends point to significant state influence. Between March 2024 and June 2025, central and state agencies directed platforms to take down roughly 1,400 posts or accounts, with a majority of notices originating from the Indian Cybercrime Coordination Centre. This volume underscores the expanding role of state institutions in moderating online content.

- Government-run Fact-Checking Units (FCUs) operate under different incentives than independent organisations. There are structural differences in mandate, accountability, and editorial independence between private fact-checking organisations and state-run FCUs, which shapes how each approaches verification and public communication.

- Questions around accountability of government FCUs remain unresolved. There is a lack of standardisation in how government FCUs respond when questionable or misleading content originates from ruling political actors, and what safeguards exist to prevent misuse of fact-checking powers for political advantage.

What next? What is the way forward?

Health Sector

- Strengthen community-level health communication

Equip local, tribal, and frontline leaders with accurate, culturally rooted health information to build preventive awareness and counter emotionally charged misinformation.

- Embed communication into healthcare practice

Provide doctors with structured tools such as verified reading material, pamphlets, and training in patient communication, to bridge the knowledge gap and address misconceptions shaped by online content.

- Meet misinformation where it spreads

Encourage healthcare professionals, public health institutions, and government programs to actively engage on digital platforms, making credible information visible, relatable, and as accessible as misleading content.

Digital Marketplaces

- Shift from reactive fixes to preventive systems

Regulators and platforms must prioritise early detection tools from self-audit mechanisms to automated checks for counterfeit logos and fake reviews to curb deceptive practices before they reach consumers.

- Strengthen digital and commercial literacy

Large-scale training programmes for MSMEs, first-time online sellers, and everyday users are essential to bridge the widening gap between online risks and public awareness.

- Increase transparency in creator and influencer ecosystems

Clear disclosure norms, accountability frameworks, and checks against paid misinformation are needed to ensure creators are not incentivised to spread unverifiable or manipulative content.

Telecom & Finance

- Prioritise nationwide scam literacy and digital hygiene education

Large-scale, community-level programmes should equip people, especially first-time digital users, with practical skills to recognise impersonation tactics, avoid high-risk behaviours, and respond quickly when targeted.

- Strengthen systemic safeguards through regulation and platform transparency

Closing KYC loopholes, improving caller traceability, and mandating regular transparency reports from platforms can create stronger deterrence and help users understand evolving fraud patterns.

- Build fraud-response networks

Collaboration among fact-checkers, cybersecurity teams, tech platforms, financial institutions and law enforcement is essential to detect emerging scams early, curb deepfake-based fraud, and support victims through faster, coordinated recovery pathways.

Policy Frameworks

- Establish standards for defining misinformation

A shared, transparent framework which is crafted collaboratively with media, civil society, technologists, and legal experts can reduce ambiguity and prevent selective or politically motivated interpretations.

- Create safeguards to separate verification from state influence

Embedding checks and balances, external oversight, and audit mechanisms can help ensure that fact-checking by government bodies does not slip into censorship or narrative control, especially during sensitive events.

- Strengthen accountability and transparency for government FCUs

Public reporting on takedown decisions, clear protocols for addressing misinformation from political actors, and standardised operating guidelines can help build trust and reduce conflicts of interest.

Conclusion

The insights shared at TIACON 2025 converge on a critical truth: Rebuilding trust and strengthening information ecosystems in the AI age demands proactive, coordinated, and context-aware responses across sectors. Whether we are confronting health misinformation, consumer deception, digital fraud, or political manipulation, a shared commitment to transparency, accountability, and community empowerment emerges as the foundation for all future efforts.

Across discussions, one theme echoed consistently—**solutions must be rooted in where people are, both geographically and digitally**. In the health sector, this means equipping community leaders with accurate, culturally relevant information and integrating communication into clinical practice. In the marketplace, it involves improving commercial literacy for small sellers and ensuring transparency in the influencer ecosystem. In finance and telecom, it calls for aggressive scam literacy campaigns and rapid, coordinated fraud-response systems. In governance, it demands frameworks that distinguish verification from control, ensuring that state-backed initiatives uphold and not erode people's freedom of expression.

Ultimately, TIACON 2025 underscored that **no single actor can safeguard information ecosystems alone**. Media, technologists, civil society, law enforcement, regulators, and everyday users must work in tandem, not only to resist harm but to actively shape a healthier digital public sphere. The work ahead is as urgent as it is shared—and it begins with showing up, showing up differently, and making the truth visible.