



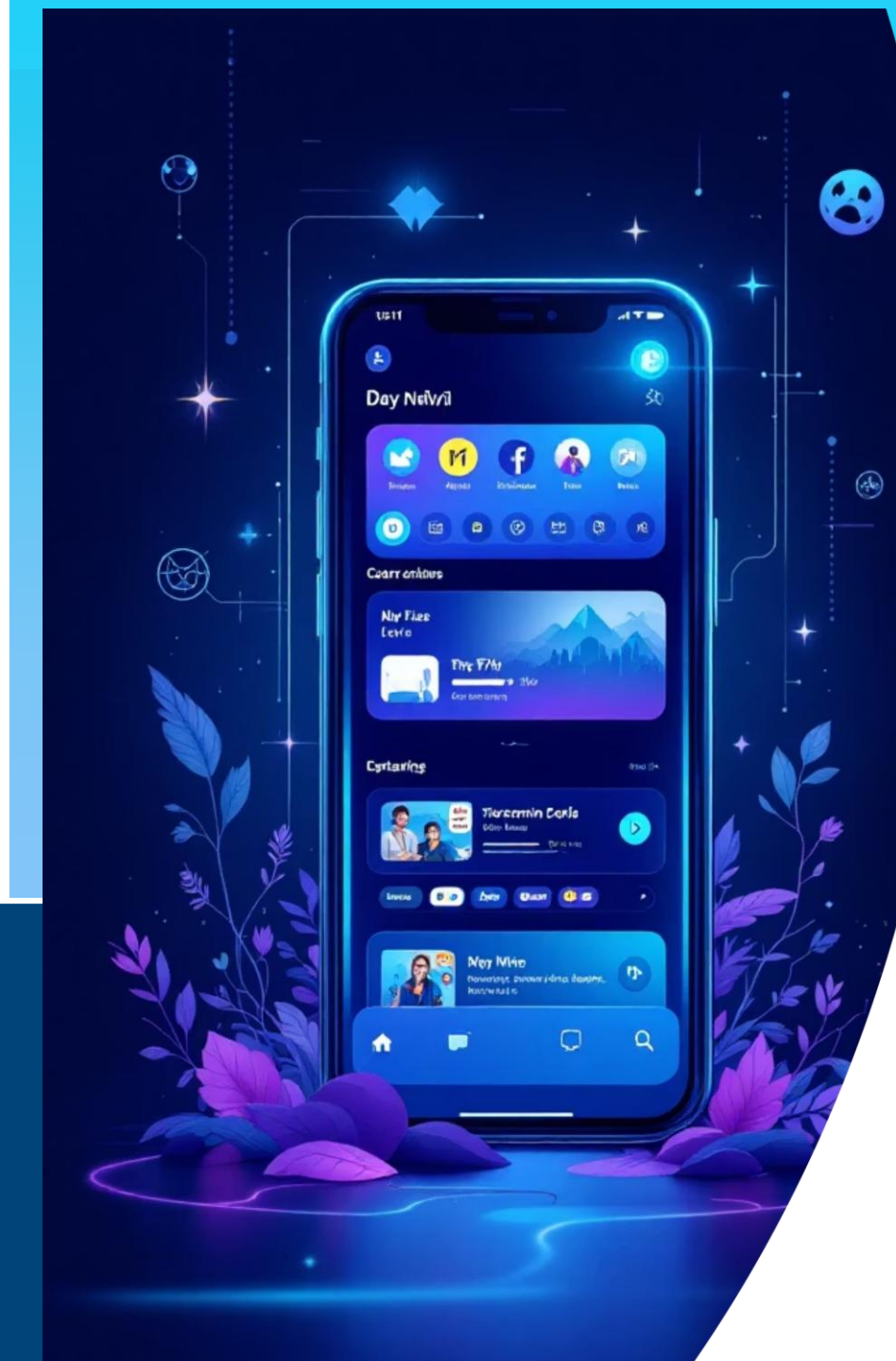
Strengthening Digital Trust- A regulatory perspective on OTT Services

OTT Workshop-Accra, Ghana

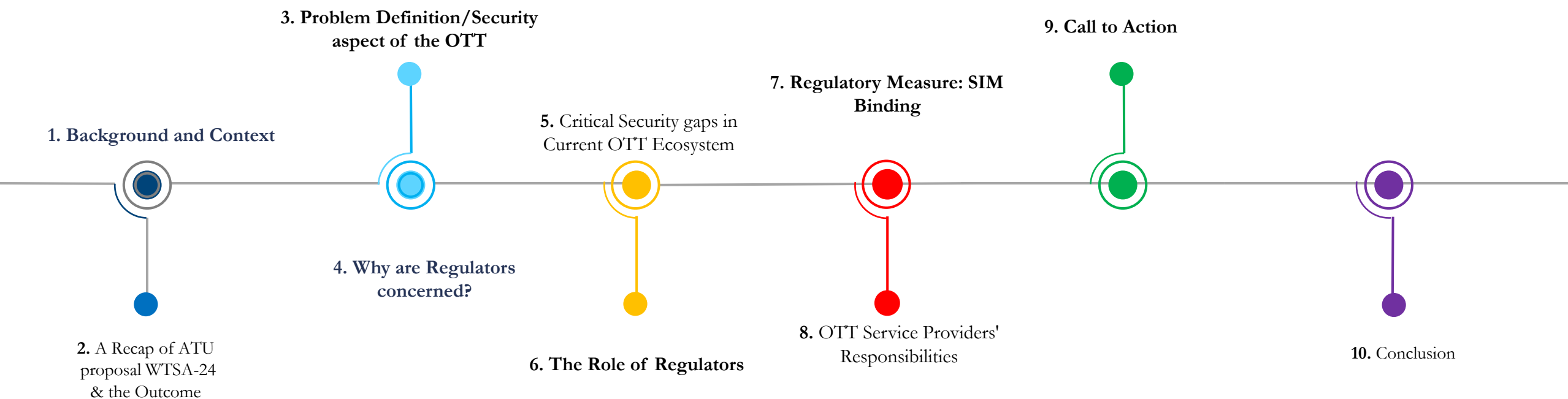


Presented by Nura Falalu
Nigerian Communications Commission

14th April 2026



Content



Background and Context

OTT platforms now play a major role in global communication, complementing traditional telecom services.

Messaging



Messaging and calling apps are now essential for individuals, businesses, and organizations.

Alternatives



Platforms like WhatsApp and Telegram have become widely used alternatives to traditional SMS and voice calls.

Digital Adoption



Rapid digital adoption has transformed how we connect but also introduced new vulnerabilities.

A Recap of ATU Proposal WTSA-24 Resolution on OTT & the outcome

The Resolution intends to achieve the following amongst others:

Government/Regulators

- National security & safety
- Innovation & Competition
- Consumer rights

Licensees/Operators

- Fair competition
- Revenue growth
- level playing field for all

Consumers

- Privacy & data security
- Quality of Experience (QoE)
- Clear complaint resolution platform

Researchers/Standard Organizations

- Protocol and standards

WTSA-24 Action OTTs

❖ *With reference to the ARB and ATU contributions, ARB/36A31/1 and ATU/35A35/1, WTSA-24, in line with Resolution 68,*

Action:

❖ *Requests the Director of TSB to convene workshops preferably back to back with relevant Study Group meetings that bring together stakeholders in the OTT ecosystem, aiming to facilitate collaboration, knowledge sharing, and consideration of diverse stakeholders' interests, while identifying and proposing innovative solutions to address their needs and interests wherever possible and report progress of workshop outcomes to TSAG.*

Security aspect of the OTTs

Government/Regulators

- National security & safety:

Problem Definition



Process

- › OTT services typically authenticate users through SIM-based verification, allowing communication over the internet. However, once users have been verified, they can continue accessing OTT applications via Wi-Fi or mobile hotspots, even without the original SIM present
- › The disconnect between **SIM cards** and **OTT accounts** weakens identity verification, allowing accounts to remain active even after SIMs are **churned**, **recycled**, **deactivated**, **removed**, or **reassigned** without further verification, thereby creating security loopholes that increase the risk of unauthorized access, misuse by third parties and **a single SIM card use by multiple users**.

- › In some instances, new SIM owners may gain unintended access to the previous owner's data on OTT accounts when phone numbers are **churned** and **reassigned**, compromising user **privacy**. This also enables the creation of **multiple or fake accounts**, which increases the risk of **scams**, **spam**, **impersonation**, and overall **misuse of mobile numbers and OTT platforms**.



Critical Security Gaps in Current OTT Usage

- › These vulnerabilities expose users and platforms to higher risks of fraud and unauthorized access, ultimately leading to a **loss of user trust**.



Unauthorized Account Usage

- › Accounts may continue to operate without re-verification even after the SIM is removed, creating a risk of unauthorized access and potential misuse by third parties.



SIM Recycling Fraud

- › New SIM owners may gain access to previous owners' messaging history and active accounts upon number reassignment.



Identity Impersonation

- › High potential for fraud and malicious activities using abandoned numbers that still have active OTT sessions.



Traceability Challenges

- › Difficulty in tracking cybercrime operations, especially when accounts are controlled from outside the local jurisdiction.

Digital Trust

Increasing user adoption of digital and why it matters

Definition

Digital trust is the confidence that people have in the security, privacy, integrity, and reliability of digital technologies and organizations.

Why it matters?

It matters because users will not adopt or engage with digital services if they feel unsafe, uncertain, or at risk of misuse or fraud.

Impact

Strong digital trust drives user confidence, business growth, and long-term resilience by ensuring transparency, ethical data use, and robust protection against cyber threats.

The Role of Regulators: Closing the Security Loop

To ensure adoption of standards that protect the digital ecosystem.

Strengthening Accountability

Introducing measures to ensure digital communication platforms are responsible for user verification.

Improving Traceability

Closing the gap between mobile identifiers and digital accounts to reduce the misuse of mobile numbers.

Verified Identity

Transitioning from "open access" to "verified identity" as the foundational requirement for communication platforms.

Mitigants

Active SIM Requirement

OTT account must be linked to an active, valid SIM card to ensure that communication always remains tied to a verified identity.

Physical Presence

The SIM card must be physically present in the device used for the OTT service.

Verification-Based Access

Account functionality depends on continuous or periodic SIM verification to prevent unauthorized use.

Regulatory Measures: SIM Binding

Device Authentication

- › Links user accounts to unique SIM card identifiers, ensuring each account is tied to a verified mobile number

Session logout

- › Requires OTT Service providers to implement device-change alert and login anomaly detection

Identity Verification

- › Requires Identity validation before and after provisioning services, creating accountability

Traceability

- › Enables authorities to identify users when legally required, balancing privacy with public safety

Why Regulatory SIM Binding Matters?

Ensure Regulatory Compliance

- › Provides consistent enforcement framework across jurisdictions. Regulators gain oversight capabilities while maintaining appropriate privacy safeguards.

Combat Digital Crime

- › Reduces spam, phishing, and fraud by eliminating anonymous accounts. Law enforcement can trace malicious actors when legally authorized, improving response to cyber threats.

Protect Vulnerable Users

- › Prevents harassment, stalking, and abuse by making perpetrators accountable. Children and at-risk populations gain protection from anonymous predators.

Build User Confidence

- › Increases trust in digital platforms by verifying participants. Legitimate users benefit from safer environments with reduced spam and malicious content.

Call to Action



Regulators

Enact mandatory Identification binding requirements through national legislation.

OTT Providers/Telcos

Commit to technical implementation and demonstrate compliance with regulatory standards.

ITU

Provide a platform and forum for deliberation among all involved stakeholders & provide technical support where applicable

Together, we can build a safer digital future where innovation thrives alongside accountability and trust.

Conclusion

Building a Safer Digital Future



Digital Trust

Strengthening trust is a prerequisite for a thriving digital economy



Traceability

Accountability and traceability are the cornerstones of a modern, secure digital landscape.



Shared Benefits

A safer ecosystem benefits all stakeholders, users, industry, and regulatory bodies alike.

- ❑ There is a need to promote a secured digital ecosystem without stifling innovation.
- ❑ A regulatory measure like SIM binding is crucial step toward reinforcing trust in our expanding digital world.



Thank You



References

A Survey on Digital Trust: Towards a Validated Definition: Julija Saveljeva & Julija Saveljeva,
Department of Management, BA School of Business and Finance, LV-1013 Riga, Latvia

Strengthening Digital Trust: DoT Introduces Mandatory SIM Binding for OTT Apps: White
Water Solutions IT Services and IT Consulting, Bengaluru, Karnataka Telecom Regulatory
Experts Specializing In Telecom Licensing And Regulatory Compliance