COMMUNIQUE

ISSUED AT THE END OF THE NIGERIA INTERNET GOVERNANCE FORUM (NIGF 2024) EVENT

NIGERIA INTERNET GOVERNANCE FORUM

N I G F

NIGERIA INTERNET GOVERNANCE FORUM

N I G F

HELD ON

OCTOBER 15 -17, 2024

Introduction

The annual Nigeria Internet Governance Forum (NIGF) facilitates fruitful partnerships and dialogue between various stakeholders, aimed at redefining the position of Nigeria at regional and global IGF meetings. The thirteenth NIGF was held as a hybrid event tagged Nigeria Internet Governance Forum (NIGF) 2024, with some stakeholders in the Nigerian Internet Community physically present at the Tamara Centre (Women Development Centre), Port Harcourt, Rivers State, Nigeria, while other participants joined virtually.

The NIGF 2024 was organised by the Nigeria Internet Governance Forum Multistakeholder Advisory Group (NIGF-MAG) which is a collaborative effort of the Federal Ministry of Communications, Innovation and Digital Economy (FMCIDE), the Nigeria Communications Commission (NCC), the National Information Technology Development Agency (NITDA), the Nigeria Internet Registration Association (NiRA), Internet Society (ISOC) Nigeria Chapter, with other Internet Stakeholders. The main event, which was held on 17th October 2024, focused on discussing the theme: "Responsible Use of the Internet: A Panacea for Sustainable Socio-Economic Development". The NIGF 2024 was preceded by the Nigeria Youth Internet Governance Forum (NYIGF) and Women Nigeria Internet Governance Forum (WNIGF) which were held in parallel on 16th October 2024.

Nigeria Women Internet Governance Forum (NWIGF): October 15, 2024.

On the 15th of October, 2024 the Centre for Information Technology and Development (CITAD) in partnership with Nigeria Internet Governance Forum held the 6th edition of the Women Internet Governance Forum (WIGF). WIGF was part of the 2024 Internet Governance Forum yearly events. The theme for this year was **Promoting a Gender-Sensitive Internet: Women Inclusivity in the Digital Transformation**.

The objectives of the forum were to:

- Discuss how to promote a gender-sensitive Internet
- Provide ways that will promote women's inclusivity in decision-making within the digital space.
- Outline strategies to tackle the challenges of women's exclusion from the Internet.
- Propose policy recommendations to address women's underrepresentation in Internet decision-making.
- Create a campaign plan to promote a gender-sensitive Internet and women's inclusivity in digital transformation.

While the aim of the 2024 WIGF was to:

Provide a discussion platform, especially among women on how to develop strategies to address issues reinforcing women's marginalization in digital transformation, and decision processes and promote a gender-sensitive Internet.

Introduction.

The keynote speaker at the 2024 WIGF was Comrade Ene Obi, the immediate past Country Director, Action Aid Nigeria. Madam Ene made her presentation on the theme for the year. Madam Mary Uduma, Chair, West Africa IGF, Aminu Naganye, Editor, WikiTimes and Ali Isah, Artificial Intelligence Research Fellow, Fact-Check Africa served as the chairs of the opening lecture and the two technical sessions that were held. The two sessions featured six speakers and discussed the following topics;

1. **Gender-Based Violence Online: Way Forward.**
2. **Promoting Internet Inclusivity: Prospects and Challenges.**

Observations:

After rigorous discussions, the participants at the forum observed the following:

- Digital Gender Gap: The disparity between men and women in accessing digital technologies remains significant. Barriers such as socio-economic factors, lack of education, limited digital literacy, cultural restrictions, and religious factors disproportionately affect women.
- Online Harassment and Cybersecurity: Women face higher risks of harassment and gender-based violence both online and offline. This often leads to reduced participation by women in the digital space, particularly in leadership roles.
- Underrepresentation of Women: Women remain underrepresented in decision-making roles, especially in technology development and policy formulation, contributing to the gender imbalance online.

- Barriers to Digital Literacy: In underserved communities, women often lack the digital literacy needed to engage fully in the online world, limiting their access to educational, employment, and social opportunities.
- Opportunities in the Digital Economy: Digital transformation offers significant opportunities for women, particularly in entrepreneurship and access to education and financial services. However, systemic biases continue to hinder women's full participation.
- Economic Barriers: High costs of Internet access, infrastructure, and digital devices prevent many women, especially those in rural communities from engaging in the digital economy.
- Cultural and Social Barriers: Cultural norms, particularly in Northern Nigeria, discourage women from pursuing careers in STEM and limit their access to technology. In some communities, men express concerns over their wives' Internet usage due to fears about negative online content.
- Technophobia and Online Harassment: A lack of familiarity with digital tools contributes to technophobia, especially in rural areas, preventing women from utilizing technology effectively. Online bullying and harassment further discourage their participation on digital platforms.
- Language Barriers: Many online platforms lack local language options, which limits rural women's ability to navigate the Internet and engage in digital spaces.
- Inadequate Government Initiatives: Previous government efforts, such as the 2019 Commission for Digital Economy initiative have not yielded substantial outcomes for gender inclusion in technology. The underrepresentation of women in government ICT leadership remains a challenge.

Recommendations.

Based on the observations made the participants recommend the following:

- Close the Digital Divide: Governments and stakeholders should invest in infrastructure and policies that ensure equal access to the Internet for women, particularly in rural areas.
- Internet Affordability: The government and other stakeholders should ensure affordable Internet access is prioritized for underserved communities.
- Safe Digital Spaces for Women: Collaboration among governments, civil society, and tech companies is essential to create stronger regulations addressing online harassment and cybercrimes targeting women.
- Platforms and web applications should be built with gender sensitivity to encourage women's participation.
- Promote Digital Literacy Programs: Education and training programs targeting women, especially those from marginalized groups, should be expanded. These could include initiatives like coding boot camps, digital marketing workshops, and financial technology training.
- Empower Women in Decision-Making: government and CSOs should Support women's participation in Internet governance through mentorship, leadership programs, and decision-making roles. This could involve deliberate mentorship programs and leadership development initiatives aimed at increasing women's influence in policy-making.
- Support Female Entrepreneurs: Governments and private sector actors should provide resources, funding, and mentorship for women in the digital economy. Creating dedicated funds or grants for women-led businesses and organizations can help close the gap.
- Enhance Rural Connectivity: Governments and private organizations should collaborate to improve Internet infrastructure in rural areas, ensuring that technological tools available in urban areas are also accessible in underserved regions.

- Mentorship and Engagement: Women should actively mentor younger girls by introducing them to business centers and digital technologies. Continuous forums like the Women Internet Governance Forum can motivate more women to assume leadership roles.
- Capacity Building in Digital Rights Protection: judiciary should be empowered to protect women's digital rights and address online harassment effectively.
- School curriculum should be updated, and digital literacy programs, including free computer distribution should target rural areas.
- Economic Support and Affordable Access: government and tech companies should provide affordable Internet and infrastructure, especially for women from low-income or marginalized backgrounds, while organizations should donate computers and offer free digital skills training.
- Policy Implementation for Digital Inclusivity: Governments must implement policies that protect freedom of speech and ensure digital inclusivity for women, persons with disabilities, and marginalized groups.
- Advocacy: groups and organizations should intensify advocacy and push for the recognition of Internet access as a right, not a privilege.
- Foster Digital Citizenship and Awareness: Public awareness campaigns should be initiated to promote responsible digital behaviors, reduce online discrimination, and promote women's rights in digital spaces.
- Language Inclusivity: To overcome language barriers, local languages should be promoted in online spaces, allowing rural women to engage more effectively in the digital environment.

Utilize Digital Centers Effectively: Underutilized digital centers in rural areas should be improved with reliable power and Internet connectivity to promote women's participation in the digital economy. A clear example of this, is the CITAD Hello World initiative.

Nigeria Youth Internet Governance Forum (NYIGF): October 16, 2024.

The 2024 Nigeria Youth Internet Governance Forum (NYIGF) was a hybrid event, combining in-person and virtual formats to maximize accessibility and engagement. The physical gathering took place in Port Harcourt, while the virtual component was hosted via Zoom, enabling nationwide participation. The event's theme, **"Navigating the Digital Sphere: Rights, Risks, and Resilience,"** positioned Nigerian youth at the center of critical discussions on digital rights, Internet safety, and technology adoption, reflecting the nation's commitment to an inclusive and secure digital future.

The Forum featured a structured program, divided into distinct sessions that catered to different levels of engagement and expertise. It opened with a high-level panel discussion where policymakers, thought leaders and digital rights advocates explored the theme's core issues. This was followed by an in-depth plenary session designed to foster open dialogue and collaborative problem-solving among participants. Additionally, the Forum dedicated a specialized session to secondary school students, offering them a unique platform to learn, share their perspectives, and engage with Internet governance topics in an accessible manner. A keynote address further highlighted the importance of youth-led initiatives in shaping Nigeria's digital landscape.

Participants actively engaged in dynamic discussions and expert-led sessions focused on strengthening resilience within Nigeria's digital ecosystem. These conversations provided an in-depth exploration of challenges and opportunities related to digital security, equitable access, and sustainable technology use. By delving into pressing issues such as cybersecurity threats, misinformation, and the digital divide, participants were able to collaboratively identify strategies to create a more inclusive, secure, and adaptable digital environment. The expertise

shared by industry leaders and digital rights advocates enriched the dialogue, empowering attendees with the insights and tools needed to drive meaningful change in Nigeria's evolving digital landscape.

The Forum successfully gathered a diverse array of stakeholders, including representatives from government agencies, academic institutions, industry professionals, and emerging Internet governance enthusiasts. This broad participation underscored the multi-stakeholder approach necessary for effective digital policy development. By bringing together these varied perspectives, the 2024 NYIGF fostered a collaborative environment where Nigerian youth were empowered to drive conversations and contribute actively to the future of Internet governance in Nigeria.

High-Level Panel Session: Navigating the Digital Sphere: Rights, Risks, and Resilience.

Key Considerations.

1. Digital Literacy and Awareness of Risks: Understanding the risks involved in engaging with digital platforms, such as cyber fraud and cyberbullying, is crucial for personal safety and well-being.

2. Protection of Personal Data: Individuals must be cautious about the kind of personal information they share online. Data shared carelessly can lead to security breaches and exploitation by malicious actors.

3. Data Protection Rights: People have digital rights, including the ability to consent to data collection (opt-in) and the right to withdraw consent (opt-out). These rights help individuals maintain control over their personal data and its use by third parties.

4. Vulnerability of Digital Footprints: Leaving traces of personal data in digital spaces can expose individuals to malicious use. Protecting digital footprints is key to preventing identity theft and other online threats.

5. Regulatory Framework: The Nigerian Data Protection Commission (NDPC) plays a critical role in regulating data protection and privacy, ensuring that individuals' rights are respected in digital spaces.

Recommendations.

1. Enhance Digital Literacy Programs: There is a need to educate individuals, especially in vulnerable groups, about the digital risks they may encounter. Cybersecurity education should be integrated into digital literacy initiatives to empower people to navigate the online world safely.

2. Be Cautious with Personal Data Sharing: Individuals should carefully consider the data they share online and assess the potential repercussions of disclosing personal information. Limiting the exposure of sensitive data can mitigate risks such as identity theft and privacy breaches.

3. Report Data Breaches and Privacy Violations: In the event of a data breach or privacy invasion, individuals should report the incident to the Nigerian Data Protection Commission (NDPC) promptly. Taking immediate action helps to mitigate further damage and ensures that malicious actors are prevented from exploiting personal data.

4. Take Preventive Measures in Case of Data Breach: If hackers gain access to personal information, individuals should first take steps to secure their data (e.g., taking down databases) to prevent further manipulation. Reporting the breach to relevant authorities before notifying the NDPC can help mitigate the risk of further exploitation.

5. File Detailed Reports: When reporting data breaches, individuals should document all evidence and actions taken to mitigate the issue. This helps authorities understand the situation and provides a clear record for investigation and resolution.

From the different breakout sessions of the NYIGF 2024, the following key

observations and recommendations were made:

Plenary Session: Empowering the Digital Generation: Addressing Challenges and Harnessing Opportunities.

Key Considerations.

- Lack of Awareness and Understanding of DPI: Many young people struggle with comprehending how Digital Public Infrastructure (DPI) functions, which can result in missed opportunities and increased privacy risks.
- Ethical Use of DPI: Leveraging DPI responsibly involves aligning its use with personal and professional goals, promoting inclusivity, ensuring transparency, and respecting data privacy in all interactions with digital platforms.
- Data Protection and Privacy: In an era of emerging technologies like AI, IoT, and Blockchain, safeguarding personal data is essential. Ethical responsibility is crucial when using these technologies, as privacy is often unintentionally compromised.
- Content Creation and Privacy Balance: There is a need for content creators to establish clear boundaries between their personal and professional lives. Being strategic in content sharing and minimizing one's data footprint can help protect privacy while pursuing career goals.

- Slow Adoption of DPI: While Digital Public Infrastructure such as NIN, BVN, and NIBSS exists, their full adoption and implementation across the country are still in progress. This slow pace impacts access to services and the effectiveness of these systems.
- Ethical Digital Transformation: Ethical considerations should always be prioritized in digital transformation, ensuring that technology development benefits society and reduces the risk of harm. Support for local platforms can mitigate data privacy concerns tied to foreign-hosted services.

Recommendations.

- Enhance Awareness and Education on DPI: To empower the digital generation, there is a need for better awareness about how DPI functions and its benefits. Educational campaigns and resources should be created to inform young people and encourage them to fully engage with these infrastructures.
- Promote Ethical Digital Practices: Young people should be encouraged to use DPI ethically, by aligning their usage with long-term career and personal goals, promoting inclusivity, and ensuring transparency. Privacy should always be prioritized, and digital interactions should be deliberate and mindful.
- Strengthen Data Privacy Protections: Emphasize the importance of data protection, particularly in the context of AI and IoT. It is crucial to build privacy-conscious habits and be cautious when sharing personal data, especially when interacting with unfamiliar platforms.
- Encourage Privacy-Conscious Content Creation: Content creators should be advised to establish clear boundaries between their personal and professional lives and be intentional about the content they share. This helps strike a balance between career advancement and privacy protection.

- Accelerate DPI Adoption: To improve access to essential services, efforts should be made to speed up the adoption and implementation of DPI systems like NIN, BVN, and NIBSS. The government and private sectors should collaborate to increase the reach and impact of these infrastructures.
- Support Local Digital Solutions: Encourage the development and adoption of indigenous platforms that meet local needs while safeguarding data privacy. This can mitigate the risks of relying on foreign-hosted services and enhance the overall effectiveness of Digital Public Infrastructure in the country.

Fireside Chat: Empowering Teens: Safety, Rights and Strength (Teen Session).

Key Considerations.

- Digital Literacy and Safety: Teenagers need to develop essential skills to use digital tools responsibly. This includes recognizing online risks such as cyberbullying, fraud, and inappropriate content.
- Impact of Excessive Internet Use: Overuse of the Internet can harm mental health, academic performance, and social skills. It's crucial to promote a healthy balance between online and offline activities.
- Online Risks and Fraud: Teenagers are increasingly targeted by fraudsters using tactics like phishing and fake deals. Educating them on how to spot malicious links and adopt security measures like strong passwords and multi-factor authentication is key.
- Cyberbullying Awareness: Cyberbullying can have severe emotional effects, such as depression or self-isolation. It’s important for teenagers to report any incidents and seek support from trusted adults.

- Parental and Educational Role: Parents should monitor their children's online activity, while teachers can reinforce digital literacy and responsible Internet use.
- Growing Internet Access Among Youth: As more young people access the Internet, there is an increasing need to protect them from online threats such as cyberbullying, privacy breaches, and exposure to harmful content.
- Role of Education: Schools play a vital role in educating children and teens about online safety, legal implications of online behavior, and digital literacy. Students should be aware that their online actions can have real-world consequences, such as legal penalties for cyberbullying or hacking.
- Collaboration Across Stakeholders: Schools, parents, tech companies, legal experts, and government bodies must collaborate to create a comprehensive approach to online safety for young people. This includes workshops, awareness campaigns, and creating a safe online environment through appropriate regulations and tools.
- Children and Teens' Voice in Policy Development: Engaging young people in the creation of policies that affect their online safety is crucial. Their firsthand experience provides valuable insights into how to improve digital rights and safety measures.

Recommendations.

- Promote Digital Literacy: Equip teenagers with the knowledge to navigate the digital world safely, recognizing risks and protecting their privacy.
- Encourage Responsible Internet Use: Foster ethical behavior online, emphasizing the importance of respecting others' rights and privacy.
- Set Boundaries on Screen Time: Implement limits on screen time, prioritize educational content, and encourage offline activities for balanced development.

- Combat Cyberbullying: Create supportive environments where teenagers can discuss online issues and encourage them to report cyberbullying incidents.
- Protect Against Online Fraud: Educate teens on how to identify scams and verify online offers to safeguard their personal information and finances..
- Educational Initiatives and Workshops: Schools should integrate digital literacy and online safety into the curriculum, covering topics like the legal implications of online misconduct, privacy violations, and the consequences of cyberbullying.
- Increased Parental Engagement: Parents should set up parental controls and maintain an active dialogue with their children about their online experiences. Schools can facilitate parent-teacher meetings focused on helping parents understand the risks and privacy issues their children might face online.
- Collaborative Approach with Tech Companies: Schools should work with tech companies to implement safety features on social media and gaming platforms that cater to young users. This can include reporting systems for inappropriate content and enhanced privacy settings for children and teens.
- Policy Advocacy and Legal Protections: Schools, in collaboration with government bodies like the Nigerian Communications Commission (NCC), should push for stronger laws that protect young people from online threats. Advocacy campaigns should aim to raise awareness about existing laws such as the Cybercrime Act and emphasize the legal risks associated with online misconduct.
- Youth Involvement in Policy Development: Establish youth-led digital advocacy groups and involve students in discussions about online safety and digital rights. These groups can be consulted during the creation of new policies or regulations regarding digital behaviour and safety.

- Empowerment through Peer-Led Programs: Encourage the formation of student-led digital safety clubs or ambassadors who can educate their peers on responsible online behaviour. These programs can be supported by schools and advocacy organizations to spread awareness of digital rights and safety.
- Leveraging Technology for Participation: Use digital tools like surveys, discussion forums, and apps to gather feedback from students on online safety policies. These platforms can ensure that young people, especially those in remote areas, have an opportunity to voice their opinions.

NIGF 2024 Event: October 17, 2024.

The theme for the NIGF 2024 was "Responsible Use of the Internet: A Panacea for Sustainable Socio-Economic Development". The NIGF addressed the following subthemes:

(i) Cybersecurity, Data Protection, and Child Online Safety as Foundations for Responsible Use of the Internet.
(ii) Emerging Technologies: Leveraging AI, IoT, and Blockchain for Responsible Internet Use.
(iii) Enhancing Multistakeholder Digital Cooperation: Internet Governance, Regulations and Infrastructure.
(iv) Digital Transformation of the Economy: Empowerment through Literacy and E-Commerce.

The Chairperson of the Nigeria Internet Governance Forum Multistakeholder Advisory Group (NIGF-MAG) and Director of eGovernment Development and Regulation at the National Information Technology Development Agency

(NITDA), Dr. Wariowei D.S., delivered the welcome address. Dr. Wariowei highlighted the forum's theme, "Responsible Use of the Internet: A Panacea for Sustainable Socio-Economic Development," emphasizing the need for inclusive, cooperative approaches to address Nigeria's digital challenges. He acknowledged the NIGF's role in fostering open dialogue and collaboration across sectors to navigate complex issues like cybersecurity, digital rights, and adaptive policies in a rapidly evolving technological landscape.

Expressing confidence in the discussions that would take place at NIGF 2024, Dr. Wariowei emphasized the potential for these dialogues to inform regulatory frameworks, strengthen cybersecurity, and support emerging technologies. He assured that the forum's recommendations would be shared broadly with academia, policymakers, and industry leaders to drive positive change and contribute to a secure, inclusive, and innovative digital environment in Nigeria. Dr. Wariowei concluded his address by encouraging active participation, urging attendees to share their expertise and collectively shape a forward-looking Internet governance framework that supports Nigeria's socio-economic growth.

Mrs. Mary Uduma, West Africa IGF Coordinator, spoke about her commitment to Internet Governance, driven by a desire to ensure that all regions in Nigeria, including the South-South and Rivers State, benefit fully from the Internet. She stressed the importance of responsible Internet use, acknowledging its integral role in daily life, impacting banking, education, communication, and more. Mrs. Uduma noted the Internet's dual nature, offering opportunities but also posing risks like privacy concerns and cybersecurity threats. She emphasized the need for West Africa to be active in global digital developments to drive economic growth in sectors like e-commerce, agriculture, and education, while underscoring the need for responsible engagement at all levels, from youth to government.

She further expressed optimism that discussions at the forum would yield actionable recommendations for stakeholders across West Africa and Africa. She highlighted the importance of multi-sectoral engagement, including government, ECOWAS, the technical community, academia, civil society, and the private sector, to implement these recommendations for the region's socio-economic advancement. In closing, she affirmed Nigeria's commitment to the annual IGF gatherings and underscored the forum's impact on both regional and global Internet policy.

Mr. Adesola Akinsanya, President of the Nigeria Internet Registrations Association (NiRA), described the forum's theme as timely and essential. He emphasized the Internet's pervasive influence on life, from commerce and education to healthcare and governance, underscoring the responsibility of all users to engage meaningfully and responsibly online. He reiterated NiRA's commitment to supporting a secure and open Internet that fosters innovation while protecting users, with the .ng domain name as a crucial element of Nigeria's digital identity.

Mr. Akinsanya also stressed that sustainable socio-economic development requires responsible Internet usage, which includes promoting cybersecurity awareness, enhancing digital literacy, and developing policies that safeguard privacy and free expression. He called for collaborative efforts among government, corporate entities, civil society, and educators to foster a safe, inclusive digital environment. Concluding, he urged participants to champion a secure Internet that drives Nigeria's economic growth and social progress.

Delivering a goodwill message on behalf of Mr. Kashifu Inuwa Abdullahi, the Director General of NITDA, Mr. Bernard Ewah emphasized the transformative power of the Internet, comparing it to landmark achievements like the development of highways and the discovery of oil. Addressing the theme, Mr.

Ewah called for responsible engagement from all sectors, including individuals, businesses, and government entities, to harness the Internet's potential for national progress while mitigating risks. He highlighted the Internet's influence on global infrastructure and its role in fostering efficiency and development, emphasizing the need for collaborative action across all sectors.

Dr. Aminu Maida, Executive Vice-Chairman of the Nigerian Communications Commission (NCC), represented by Dr. Chris Agha of the Port Harcourt Zonal Office, emphasized the relevance of this year's theme, which aligns with the NCC's commitment to ensuring the Internet contributes to national development while addressing the challenges of the digital age. Dr. Chris praised the forum's multi-stakeholder approach and acknowledged the pre-events, such as the Nigerian School of Internet Governance, Youth IGF, and Women's IGF, for their focus on inclusivity and empowerment. He encouraged participants to work towards actionable outcomes that would shape Nigeria's Internet governance landscape, reaffirming NCC's commitment to collaborative efforts that foster responsible Internet use.

Engr. Olomiete Ayeo Enekpeni, Permanent Secretary at the Ministry of Communication, Science, and Technology, Akwa Ibom State, reflected on Nigeria's challenges in leveraging the Internet for socio-economic advancement. He underscored the need for a shift in mindset towards responsible Internet use, especially in sectors such as politics, family life, and the economy. Engr. Enekpeni stressed that while the Internet has the potential to provide economic opportunities, irresponsible usage could exacerbate issues like unemployment and inequality. He called on individuals, particularly parents, to take personal responsibility in guiding youth toward productive online engagement, highlighting the collective role in shaping Nigeria's digital future.

Engr. Faruk Yusuf Yabo, Permanent Secretary of the Federal Ministry of Communications, Innovation, and Digital Economy, underscored the ministry's commitment to fostering a digitally inclusive Nigeria. He outlined achievements like the National Broadband Plan, which has increased broadband penetration from 6% in 2015 to nearly 50% in 2023, with a target of 70% by 2025, and the Nigerian Startup Act, which supports Nigeria's growing tech ecosystem. Engr. Yabo emphasized the importance of ethical online behavior, data protection, and digital citizenship, inviting stakeholders to collaborate on frameworks that promote responsible Internet use.

On behalf of the Ministry of Women Affairs and the Rivers State Government, Dr. Roselyn Uranta expressed gratitude to the organizers of the Nigeria Internet Governance Forum (NIGF) and acknowledged the importance of the forum's theme, "Responsible Use of the Internet." She emphasized the critical role the Internet plays in everyday life, noting that while some individuals use it positively for research, business, and knowledge acquisition, others misuse it for fraudulent and unethical purposes. Dr. Uranta highlighted the need for greater sensitization to promote responsible and ethical Internet usage, stressing that programs like the NIGF are essential for fostering awareness and capacity-building among users.

The ceremony concluded with a vote of thanks from Engr. Kunle Olorundare, President of the Internet Society Nigeria Chapter. He acknowledged the contributions of key dignitaries, including the Honorable Minister for Communication, Innovation, and Digital Economy, Dr. Bosun Tijani, and recognized the leadership roles played by stakeholders in addressing crucial issues within the ministry's purview. Engr. Olorundare expressed gratitude for the continued support of Mr. Adesola Akinsanya, Mr. Kashifu Inuwa Abdullahi, Dr. Aminu Maida, Engr. Olomiete, and Engr. Faruk Yusuf Yabo, along with

appreciation for the presence of Rivers State Governor Siminalayi Fubara, represented by Commissioner Dr. Roselyn Apawari Uranta.

Observations from the High-level panel session:

The following were observed during the Plenary of the 13th Nigeria Internet Governance Forum:

- Barriers to Digital Inclusion: Persistent challenges, including insufficient investment, security concerns, and neglected infrastructure, continue to obstruct digital inclusivity in Nigeria.
- Stakeholder Responsibility: There is a collective duty among stakeholders to dismantle these barriers and establish an accessible and secure digital infrastructure for all Nigerians.
- Positioning for Emerging Technologies: As new technologies reshape global industries and daily life, Nigeria is at a critical juncture to strategically position itself as either a leader or a follower in adopting these innovations.
- Economic and Social Potential of Technology: Emerging technologies present significant opportunities for economic growth, social advancement, and enhanced governance if strategically applied to address current societal challenges.
- Navigating Governance and Privacy Challenges: Stakeholders face complex challenges in adopting technology responsibly, with considerations for data privacy, security, and regulation.
- Data Proliferation and Privacy: The growth of data in the digital age necessitates a balanced approach to leveraging data while safeguarding individual privacy rights.

- Child Safety in Digital Spaces: The National Data Protection Regulation (NDPR) includes provisions on child safety online, with agencies like the NCC actively developing frameworks to ensure online protection for minors.
- Comprehensive Data Safety: It's essential not only to focus on data control and protection but also on data safety within the value chain. Regulatory practices seen in regions like the EU serve as robust models, addressing broad, global perspectives on data governance.
- Dual Challenges of Infrastructure: Infrastructure issues encompass both coverage and usage, and both aspects need attention to achieve widespread Internet adoption.
- Capacity Building Needs: The pace of Internet usage is hindered by a lack of capacity-building initiatives that would empower users with digital literacy skills.
- Engagement of Nigerian Youth: Sensitive issues are seldom addressed among Nigeria's youth, highlighting the need for open discourse and engagement to promote responsible Internet use.
- Regulatory Balance: Finding an appropriate regulatory balance will facilitate digital adoption and growth across Nigeria.
- Transparency and Inclusivity: Transparent, open decision-making processes are fundamental to ensuring inclusivity within Nigeria's digital landscape.
- Youth Engagement for Online Safety: Engaging youth in policy development can encourage responsible Internet use and help establish protective measures for minors online.
- Inclusive Regulation as Seen in the EU: Inclusive regulatory frameworks in regions like the EU have proven effective in adapting to rapid infrastructure evolution and addressing its challenges.

- Importance of Market Competition: Evolving competitive markets can enhance infrastructure coverage, customer reach, and affordability—elements essential for improving digital accessibility.
- Promoting a Safe Internet for Children: Creating a safe online environment for Nigerian children requires a multi-faceted approach involving education, technological safeguards, and stakeholder collaboration.
- Balancing Data Sharing and Privacy: Nigeria must strike a balance between the advantages of data sharing and the protection of privacy rights to support sustainable digital development.
- Collaborative Approach to Digital Infrastructure: Ensuring inclusive, accessible, and secure digital infrastructure in Nigeria necessitates a holistic approach involving government policies, private sector input, and multi-stakeholder cooperation.

Recommendations from the High-level Panel Session:

- Promoting Multi-Stakeholder Engagement: A multi-stakeholder discourse is crucial to foster responsible data management and monetization practices, building a digital ecosystem founded on integrity and accountability.
- Expanding Investment Beyond Infrastructure: Investments should go beyond infrastructure deployment to include policies that drive Internet affordability and inclusivity.
- Unified Stakeholder Efforts: Collaborative efforts among government bodies, private enterprises, civil societies, academia, and citizens are needed to amplify the collective impact on Internet governance.
- Prioritizing Cybersecurity Education: To empower Nigerian citizens for safe digital navigation, cybersecurity education must be prioritized in digital literacy initiatives.

- Championing Policies to Bridge Digital Divides: Policies that reduce digital divides should be supported, enabling equitable access and progress in the digital sphere.
- Infrastructure Access Policies: Policies such as reducing right-of-way access fees are needed to facilitate infrastructure expansion and usage.
- Adopting Emerging Technologies Safely: By embracing emerging technologies with agile regulatory frameworks, Nigeria can mitigate the associated risks. These frameworks should include safe reporting spaces supported by regulatory bodies.
- Forging Data Privacy Partnerships: Collaborative partnerships on data privacy can help maintain a balance between data utilization and protecting data owners' rights.
- Supporting Youth, Entrepreneurs, and Innovators: Nigeria's digital economy can thrive by nurturing young talent, entrepreneurs, and innovators through targeted programs and resources.
- Translating Discourse into Action: Action-oriented outcomes are essential, with each stakeholder voice representing an opportunity to shape Nigeria's digital future.
- Targeted Sensitization Initiatives: Awareness campaigns should be tailored to specific demographics, ensuring targeted outreach and relevance.
- Incorporating Capacity-Building in Education: Integrating Internet awareness into educational curricula, in partnership with academia, will help foster digital literacy from an early age.
- Implementing the Data Protection Act: The Data Protection Act under the NDPR should be enforced with accountability measures for data storage providers and handlers, supported by comprehensive policies.

Session 1: Cybersecurity, Data Protection, and Child Online Safety as Foundations for Responsible Use of the Internet.

Observations:

- Urgent Need for a Comprehensive Cybersecurity Strategy: Nigeria faces a rapidly evolving cyber threat landscape that requires a cohesive, well-defined national strategy to secure critical infrastructure, safeguard personal data, and protect citizens. This strategy must be dynamic to address both current and future digital risks.

- Challenges in Data Protection Due to Increased Cloud Usage: As cloud storage becomes more common, there are concerns over centralized data held by third parties, which can heighten vulnerabilities. Effective data protection is essential to maintain trust in digital services and requires robust policies that ensure responsible handling and protection of user data.

- Child Online Safety as a Pressing Issue: The session underscored the growing risks children face online, including exposure to harmful content, cyberbullying, and online exploitation. Protecting children in digital spaces requires greater collaboration among parents, educators, tech companies, and policymakers to create safer online environments.

- Stakeholder Collaboration Essential for Cybersecurity and Data Protection: Protecting Nigeria's digital landscape requires active collaboration across government, private sector, and civil society, with clear roles for each in cybersecurity and data protection efforts. This unified approach can enable faster, more effective responses to cyber incidents.

- Need for Public Awareness and Digital Literacy: A lack of awareness regarding cybersecurity best practices among the general public presents a significant vulnerability. The session emphasized that promoting digital literacy is crucial, as it empowers citizens to understand and mitigate cyber risks.

- Complexity of Enforcing Age Verification and Parental Controls: Implementing effective age verification and parental controls remains a challenge due to limited infrastructure and resources. However, these measures are vital to ensure that children are not exposed to inappropriate or harmful content online.

- Alignment with Global Standards: The session highlighted the importance of adopting international standards, such as ISO 27001, to guide cybersecurity practices. This alignment with global best practices will strengthen Nigeria's cybersecurity posture and enhance trust in its digital ecosystem.

- Data Privacy Balance Amid Increasing Data Proliferation: With data being increasingly generated and shared, Nigeria must strike a balance between harnessing data for innovation and ensuring the privacy rights of individuals. The session emphasized the need for policies that safeguard data privacy while enabling data-driven growth.

Recommendations.

- Develop a Comprehensive National Cybersecurity Strategy: Nigeria should establish a cybersecurity strategy that addresses both current and future digital threats. This should outline responsibilities for government agencies, private sector companies, and educational institutions to create a unified, proactive approach.

- Establish a Dedicated Cybersecurity Agency: A centralized cybersecurity agency could oversee efforts across all sectors, ensuring compliance with international cybersecurity standards and facilitating rapid response to threats.
- Adopt Global Standards (ISO 27001): Critical infrastructure and high-risk sectors, such as finance, healthcare, and energy, should adhere to ISO 27001 standards to protect sensitive data and systems. This could involve adopting schemes similar to Singapore's cybersecurity labelling, which helps consumers identify products that meet cybersecurity standards.
- Regular Cybersecurity Framework Updates: To remain effective, Nigeria's cybersecurity framework should be regularly reviewed and updated in line with evolving cyber threats, ensuring it addresses current and emerging risks.
- Create a Comprehensive Data Protection Law: Nigeria should introduce and enforce a robust data protection law that includes provisions for data privacy, user consent, and accountability. This would help establish clear guidelines for handling personal and organizational data securely.
- Mandate Age Verification Systems: Technology platforms, particularly those targeting young audiences, should be required to implement age verification mechanisms to prevent unauthorized data access by children.
- Encourage Parental Involvement: Schools and parents should be actively involved in digital safety education, providing guidance on safe online behaviours and implementing protective measures on children's devices.
- Integrate COP Curriculum in Schools: Introduce a Child Online Protection (COP) curriculum that educates children on safe Internet practices, digital literacy, and responsible online behaviour.
- Implement Age-Appropriate Content Filters: Platforms and Internet service providers should collaborate to ensure that children are only

exposed to age-appropriate content. Filters can prevent access to harmful or inappropriate material.

- Establish Reporting Systems for Child Safety Issues: Create a structured system for reporting and addressing harmful online content and behaviors affecting children, ensuring quick intervention when issues arise.
- Collaborate with Technology Companies and Social Media Platforms: Partnerships with tech companies could enhance child protection efforts by embedding safety features, such as parental controls and content moderation, directly into platforms children frequently use.
- Enact Stricter Penalties for Crimes Targeting Children Online: Introduce and enforce stringent penalties for cybercrimes targeting children, such as cyberbullying and online exploitation, to deter potential offenders and emphasize the seriousness of these offences.
- National Awareness Campaigns: Leverage media outlets and community initiatives to conduct regular awareness campaigns, including jingles, advertisements, and informational programs, to educate citizens on cybersecurity and responsible Internet use.
- Support a "Whole of Society" Approach: Encourage community leaders, educators, and organizations to promote cybersecurity knowledge at the grassroots level, engaging all demographics in safe digital practices.
- Encourage Digital Literacy Among Youth: Schools should integrate digital literacy programs that equip students with skills to recognize and avoid cyber threats, protect their personal data, and use the Internet responsibly.
- Strengthen Existing Laws and Policies: Build on the Nigerian Cybersecurity Act of 2015 by enhancing enforcement mechanisms, closing regulatory gaps, and updating it to reflect new cyber challenges.
- Involve Key Stakeholders: Policymakers should collaborate with stakeholders, including parents, educators, and tech companies, to

implement effective cybersecurity measures and ensure compliance across all sectors.

- Promote Cybersecurity as a Shared Responsibility: Encourage public participation in cybersecurity initiatives and foster a collective sense of responsibility to safeguard Nigeria's digital ecosystem.

Session 2: Emerging Technologies: Leveraging AI, IoT, and Blockchain for Responsible Internet Use.

Observations from Session 2:

- Policy Development for Emerging Technologies: Nigeria's policies for IoT, AI, and Blockchain are in the early stages, with key documents like the National Digital Economy Policy and Strategy and National AI Strategy still in draft form. The importance of finalizing and implementing these policies was emphasized to support structured growth in these sectors.
- Privacy and Security Risks: Privacy remains one of the most significant challenges for emerging technologies, particularly in relation to data protection for IoT and AI. Concerns were raised about the need to update existing frameworks, such as the Nigeria Data Protection Regulation, to address evolving threats.
- Infrastructure and Capacity Building: The need for robust digital infrastructure, including 5G, and capacity-building programs is critical to support IoT and AI deployment. Investing in these areas is essential for responsible and efficient technology adoption across Nigeria.
- Stakeholder Education and Public Awareness: There is a gap in public knowledge about emerging technologies and their impact. Increased awareness campaigns are needed to educate citizens on IoT and AI, including the benefits and associated risks, particularly around data privacy.

- Blockchain Regulation and Experimentation: Blockchain adoption in Nigeria, especially within fintech, highlights a need for regulatory frameworks that balance innovation with security. Stakeholders suggested that controlled experiments with blockchain applications can provide insights and help shape regulatory approaches.
- Inclusive Growth and Local Development: Emerging technologies like AI, IoT, and blockchain present opportunities for inclusive growth across sectors such as agriculture and finance. However, realizing this potential requires fostering local capacity to create technology solutions that address Nigeria's unique challenges.

Recommendations from Session 2:

- Formalize Draft Policies and Frameworks: Expedite the transition of draft policies on AI, IoT, and blockchain to formal documents with clear timelines and actionable steps for implementation.
- Strengthen Data Privacy Regulations: Amend and update data protection laws to address emerging privacy risks. Specifically, enforce regulations that protect citizens' data from unauthorized sharing and enhance cybersecurity measures across digital platforms.
- Invest in Digital Infrastructure and Education: Prioritize investment in infrastructure like 5G networks to support IoT and AI applications, and establish educational initiatives to increase digital literacy and technological competency among all age groups.
- Promote Public Awareness on Data Privacy: Launch campaigns to educate citizens about the importance of data privacy and security practices, including reading app terms and conditions thoroughly before sharing personal data.

- Develop Regulatory Frameworks for Blockchain: Establish regulatory guidelines for blockchain technology, with an emphasis on controlled pilot programs to monitor and assess its impact within sectors like finance and logistics.
- Encourage Multi-Stakeholder Collaboration: Foster public-private partnerships to ensure diverse stakeholder input in policy formulation, thus enhancing support for innovation while ensuring technology development aligns with public interest.
- Advance Inclusive Growth through Local Capacity-Building: Implement programs focused on building local skills to develop IoT, AI, and blockchain solutions, fostering a self-sustaining technology ecosystem that supports Nigeria's socio-economic needs.

Session 3: Enhancing Multistakeholder Digital Cooperation: Internet Governance, Regulations and Infrastructure.

Observations from Session 3.

- More emphasis should be given to the development of infrastructure capacity in Nigeria.
- Role of internet governance in sustainable development.
- Data from NBS showed that 77% of youth have gained skills through internet use.
- It is important to set standards to address the digital divide in the country.
- NCC and NITDA to organize advocacy programs and digital skills training for youths.
- Federal policies and regulations on right-of-way charges at the state level should be implemented.

Recommendations

- Establish and carry out capacity-building programs to improve stakeholders' knowledge, especially in the areas of internet governance and digital infrastructure at the federal and state government levels.
- State governments should be encouraged to adopt and implement national digital inclusion programs to ensure consistency and effectiveness across the country.
- A robust regulatory framework that protects users' interests and promotes responsible use of the internet should be developed.
- Promote sustainable practices in digital infrastructure development to ensure long-term benefits and minimize environmental impact.
- Collaboration should be promoted among stakeholders and operators to invest in and deploy digital infrastructure, especially in underserved and rural areas.
- Stakeholders and Government should develop and promote digital literacy awareness initiatives, and online safety education programs, starting from the grassroots, and provide orientation on digital tool usage in workspaces, organizations, and MDAs.
- The government and stakeholders should enhance Cybersecurity and Data Protection, enforce data protection laws, review and update cybersecurity frameworks.
- The government and stakeholders should ensure Child Online Safety, encourage parental involvement, implement parental controls, implement age verification systems, and enact laws to punish offenders.

For further information, please refer to the full NIGF 2024 Report on the NIGF website: www.igf.ng or contact the Desk Officer, NIGF Secretariat via desk@nigf.org.ng.