#AdLegal

BTA SUMMIT
AFRICA BIG TECH ACCOUNTABILITY SUMMIT 2026
Kampala, Uganda

Summit Report

Big Tech & Data Privacy Enforcement in Africa

Africa Big Tech Accountability Summit

30 July 2026 | Kampala, Uganda

info@adlegalug.com

Background

The Africa Big Tech Accountability Summit (BTA Summit) 2026 was held in Kampala, Uganda, on 30–31 July 2026 under the broader theme *"Big Tech, Data Governance, and Competition Policy in Africa's Digital Economy."*

The first day of the Summit, held on 30 July 2026, focused specifically on Big Tech and data protection in Africa. It brought together data protection regulators, privacy practitioners, policymakers, lawyers, academics, civil society representatives, technology experts and other stakeholders to examine the growing challenges associated with the collection, use, sharing and governance of personal data by global technology companies operating across African markets.

The Summit provided a platform to examine the practical challenges faced by African regulators and other stakeholders in ensuring compliance with data protection and privacy laws, including questions of jurisdiction, cross-border data transfers, regulatory cooperation, consent, transparency, accountability and access to effective remedies.

Particular attention was given to the practical experience of African data protection authorities in investigating and enforcing data protection obligations against Big Tech companies.

This report presents the key discussions, interventions, experiences and lessons arising from Day One of the BTA Summit 2026, with particular focus on the evolving landscape of Big Tech, data protection and privacy accountability in Africa.

The Summit At a Glance

20+ Speakers, Panelists and Moderators drawn from Africa, Europe and other jurisdictions	**231** **Total Participants** 41 (17.7%) Physical 190 (82.3%) Online
05 **Thematic Sessions** Panel Sessions 1 Keynote Address	**09** **Hours** Sessions and working

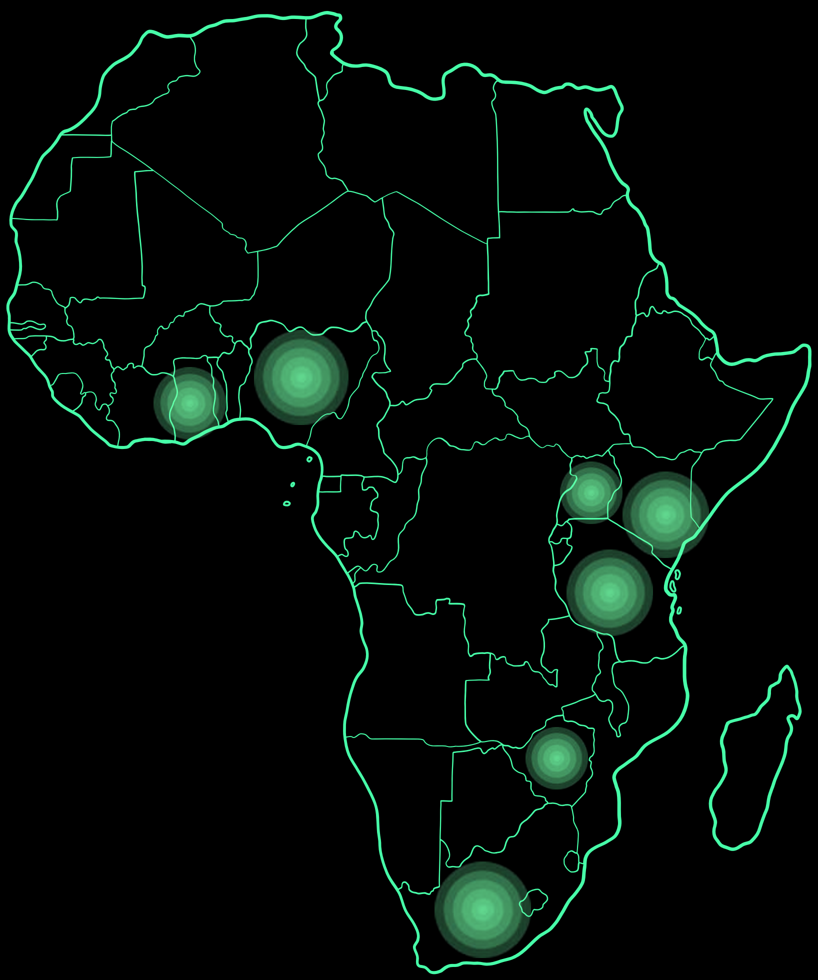
What We Set Out To Do:

- Strengthen Big Tech privacy accountability in Africa.
- Improve enforcement capacity against Big Tech data practices.
- Advance cross-border privacy cooperation among African regulators.
- Empower civil society to drive privacy advocacy and accountability.
- Strengthen Africa's data protection community through collaboration and knowledge sharing.
- Promote African-centred approaches to Big Tech data governance.
- Strengthen African privacy remedies and judicial capacity for affected data subjects.
- Promote responsible Big Tech data practices through transparency, consent and privacy by design.

Geographical Reach

Connecting Africa on Data Protection & Big Tech Accountability

The Africa Big Tech Accountability Summit 2026 brought together a diverse African community of regulators, data protection practitioners, policymakers, civil society representatives, academics, technology experts and media professionals. With participation and expertise drawn from across the continent, the Summit provided a truly pan-African platform for cross-border dialogue, knowledge exchange and collective reflection on data privacy, digital rights and Big Tech accountability in Africa.



Geographical Region	Countries Represented
Africa	**West Africa** — Nigeria, Ghana **East Africa** — Kenya, Uganda, Tanzania **Southern Africa** — South Africa, Zimbabwe


BTA
SUMMIT
THE AFRICA BIG TECH
ACCOUNTABILITY SUMMIT 2026
Kampala, Uganda

Keynote Address:

Whose Data, Whose Law? Jurisdiction, Extraterritoriality, and Enforcement Against Offshore Big Tech Platforms in Africa

Olumide Babalola, PhD

Chairperson, Nigeria Bar Association Data Protection Committee
Founder, Data Privacy Lawyers Association of Nigeria
Managing Partner, Olumide Babalola LP

"Before 2024 or 2025 the Big Techs were not really taking Africans seriously. But now, with successful cases and growing legal challenges across the continent, African courts, regulators and lawyers are demonstrating that these companies are not unreachable." - *Dr. Olumide Babalola*

Dr. Olumide's keynote focused on the difficulty of holding offshore Big Tech platforms accountable for data protection violations affecting African users. He highlighted the central paradox that the data belongs to Africans, yet the servers, corporate structures and much of the legal infrastructure governing that data are located outside Africa. This creates serious challenges for African courts, regulators and individuals seeking effective remedies.

He explained that while African data protection laws increasingly contain extraterritorial provisions, allowing countries to regulate companies outside their territories where they process or target the data of people within those countries, the greater challenge is enforcement. A court may have jurisdiction to issue an order, but enforcing that order against a company with no local office, assets or representative can be extremely difficult.

Dr. Babalola argued that Big Tech companies have developed corporate and contractual structures that make accountability difficult. These include the absence of local offices, foreign choice-of-law provisions, requirements to litigate in foreign jurisdictions, complex corporate structures and offshore data storage. Such arrangements create significant financial and practical barriers for African users seeking justice.

Drawing on litigation involving Meta, Google and Twitter/X, particularly in Nigeria, he demonstrated that African courts and regulators can successfully hold global technology companies accountable. However, he stressed that winning a judgment is not necessarily the same as obtaining a remedy, particularly where the judgment cannot be enforced against the company or its assets.

The keynote also examined the particular African context of data protection. Dr. Babalola noted that economic vulnerability can make individuals more willing to surrender personal data in exchange for relatively small financial benefits. He used the Worldcoin experience in Kenya to illustrate the risks associated with collecting sensitive biometric information from economically vulnerable populations.

Key Themes of the Keynote Address:

1. The African Data Paradox

Dr. Babalola highlighted the fundamental paradox that African users generate and provide the data, while the infrastructure, servers and corporate entities processing that data are predominantly located outside Africa. This disconnect creates significant challenges for African regulators and courts seeking to exercise effective control over African data.

2. Jurisdiction and Extraterritoriality

A central theme was the growing use of extraterritorial data protection laws. While African countries can regulate offshore platforms that process the data of or target users within their territories, the critical challenge remains translating legal jurisdiction into practical enforcement.

3. The Enforcement Gap

The keynote emphasised that obtaining a judgment against Big Tech does not necessarily result in an effective remedy. The absence of local offices, assets and representatives makes service, execution and recognition of judgments particularly difficult. As Dr. Babalola stressed, a judgment can become effectively meaningless if it cannot be enforced.

4. Big Tech's Structural and Contractual Advantage

Dr. Babalola examined how Big Tech companies use foreign choice-of-law clauses, jurisdiction provisions, complex corporate structures and offshore infrastructure to make themselves difficult to reach through African legal systems. These arrangements create a major imbalance between multinational platforms and individual African users.

5. The African Context of Data Protection

The keynote questioned the practice of simply importing European data protection concepts into African legal systems without adapting them to African social, cultural and economic realities. He argued that African countries must develop approaches that respond to their own circumstances rather than relying entirely on copy-and-paste regulation.

6. Poverty, Data and Digital Vulnerability

Dr. Babalola connected data protection with Africa's broader socioeconomic realities. Economic vulnerability can lead individuals to exchange valuable personal information for relatively small financial benefits, demonstrating why data protection must also be understood within the context of poverty, inequality and digital dependency.

7. Consent and Unfair Digital Contracts

Another major theme was the weakness of conventional "click-to-accept" consent. Dr. Babalola argued that genuine consent must be voluntary, specific and informed, and that platforms should be able to demonstrate what users actually agreed to and how their data would be used.

8. Strategic Litigation as a Tool for Accountability

The keynote presented litigation as an important mechanism for developing African data protection jurisprudence. Successful cases against Big Tech can establish precedents, encourage other litigants and demonstrate that global technology companies are not beyond the reach of African courts.

9. Stronger Regulatory and Institutional Capacity

Dr. Babalola identified inadequate funding, staffing and technical expertise as major obstacles facing African data protection authorities. Strengthening regulators is therefore essential if extraterritorial laws and regulatory powers are to translate into meaningful enforcement.

10. African Regional Cooperation

The keynote strongly advocated for greater cooperation among African countries, including regional approaches to enforcement, recognition of judgments, cross-border data governance and regulatory coordination. He argued that Africa must develop collective leverage when dealing with multinational technology companies.

11. Data Sovereignty and Local Representation

Dr. Babalola called for African countries to consider data localisation, data sovereignty and requirements for Big Tech companies to maintain local or regional representatives. Such mechanisms would provide regulators and users with more accessible channels for accountability.

12. Building an African Digital Regulatory Model

The keynote ultimately called for Africa to move beyond fragmented national regulation and develop a coordinated model of digital accountability that reflects African realities. His closing message was that African data protection must evolve from laws that exist on paper into systems capable of producing real remedies and meaningful accountability against global technology platforms.

Central Message

The keynote's central message was that African data protection cannot stop at obtaining laws, regulatory decisions or court judgments; the real test is whether African institutions can secure effective remedies against global platforms. Dr. Babalola called for African jurisdictions to move from fragmented national approaches toward greater regional cooperation, stronger enforcement mechanisms, local representation of Big Tech, institutional capacity-building and the development of African jurisprudence suited to African realities.

He concluded with a particularly important observation for the summit: African privacy and data protection law will be shaped not only by legislation, but by strategic litigation and the cases that African lawyers are willing to bring. He noted that some cases will fail, but successful cases can establish precedents that reshape the industry and encourage other African courts and litigants to hold Big Tech accountable.


BTA SUMMIT
30-31 JULY 2026
THE AFRICA BIG TECH ACCOUNTABILITY SUMMIT
Kampala, Uganda
SUMMIT THEME: Data Protection, Competition, and the Future of Africa's Digital Economy
East African Community Competition Authority
ECOWAS Regional Competition Authority
DPO PRIVACY CENTRE EAST AFRICA
Kirunda & Co. ADVOCATES
DIGITAL LAW HUB
ADCF

#AdLegal

SESSION ONE | REPORT

Inside the Investigation Room: How African Data Protection Authorities Took On Big Tech

About the Session:

The Session brought together practical experiences from across Africa on how regulators and legal practitioners have confronted the growing data protection challenges presented by major technology platforms. The session featured a Ugandan data protection regulator who shared first-hand experience handling investigations involving major Big Tech companies, including Google, Meta and WhatsApp, and explained the practical realities of complaints, investigations, jurisdiction, evidence gathering, regulatory orders and post-decision compliance.

The session also drew on Kenya's experience, including regulatory and public interest concerns surrounding TikTok and the broader challenges of protecting users while balancing privacy, freedom of expression and online safety.

From Nigeria, the discussion brought the perspective of a leading data protection lawyer involved in the country's landmark Big Tech privacy enforcement experience, including the investigation and significant penalty imposed on Meta.

Across these experiences, the session demonstrated how African authorities are increasingly moving from theoretical regulation to active enforcement and accountability of global technology companies, while confronting common challenges such as cross-border jurisdiction, limited institutional capacity, public awareness and the need for stronger cooperation across African jurisdictions.

Speakers:

Baker Birikujja
National Personal Data Protection Director (Uganda)

Speaker

Dr. Olumide Babalola
Founder, Data Privacy Lawyers' Association of Nigeria

Speaker

Irene Makau
The Oversight Lab Africa

Speaker

Jasper Twesige
Cavenbridge Advocates

Session Chair

Speaker Submissions

Baker Birikujja

National Personal Data Protection Director (Uganda)

Mr. Birikujja provided a practical account of how Uganda's Personal Data Protection Office receives, investigates and enforces complaints involving Big Tech and other data controllers.

He explained that the Office applies a standardized complaints and investigations process regardless of the size of the respondent, while giving particular priority to complaints involving significant public interest, large numbers of affected data subjects or serious potential harm.

He also highlighted the practical challenges of regulating global technology companies that have no physical presence in Uganda, particularly in establishing jurisdiction, identifying the appropriate representatives and obtaining timely responses.

At the same time, his experience with Google, Meta, WhatsApp and OpenAI demonstrated that well-reasoned regulatory decisions can ultimately produce meaningful compliance and behavioural change.

Key pointers from Mr. Birikujja's presentation:

- Big Tech complaints follow a standardized regulatory process. The Personal Data Protection Office applies its complaints and investigations manual to both small companies and major technology companies. Complaints are first assessed for legal relevance. The Office determines whether the complaint concerns conduct governed by the Data Protection and Privacy Act and whether there is an alleged breach or violation.
- Public interest influences prioritisation. Complaints affecting large numbers of data subjects or involving significant potential harm receive greater priority during the Office's triage process.
- The first Big Tech complaint involved Google and the second involved Meta and WhatsApp. The investigation primarily concerned cross-border data transfers and registration.
- Jurisdiction presents a major challenge. Global technology companies such as Google, Meta and WhatsApp may operate extensively in Uganda without maintaining physical premises in the country.
- Identifying the appropriate respondent can delay investigations. Regulators may need to determine not only where a company is located but also which person, office or department has authority to respond to the complaint.
- Global corporate structures create practical delays. Decisions within large technology companies may involve personnel across different countries, time zones, working cultures and internal processes.
- Regulators must balance speed with procedural fairness. Although complainants expect investigations to be completed within statutory timelines, the Office avoided simply proceeding in the absence of the respondent because it considered it important to give the affected company a proper opportunity to be heard.
- Enforcement does not end with a decision. Birikujja stressed that "being a regulator is not just about issuing a decision". The ultimate objective is to change behaviour, establish compliance and ensure that regulatory orders are implemented.
- Big Tech can cooperate when the right channels are established. From his experience, companies may become responsive once regulators identify the appropriate offices and communicate clearly what is required.
- Google eventually registered with the Ugandan regulator and provided documentation relating to the regulatory orders issued against it.
- Meta and WhatsApp also implemented the orders issued by the regulator. This included establishing a Uganda-facing privacy notice reflecting Ugandan requirements. Meta and WhatsApp also developed mechanisms requiring users to actively consent before linking or sharing data across services such as WhatsApp, Facebook and Threads.
- Well-reasoned regulatory decisions can encourage voluntary compliance. Birikujja observed that Big Tech companies were more willing to address identified deficiencies where the regulatory process was objective, the evidence properly assessed and the requirements clearly explained. Effective Big Tech accountability requires decisions that are supported by evidence, clearly identify the deficiency and explain what the respondent is required to do.
- Regulatory cooperation should focus on implementation. Engagement with Big Tech should not end at the investigation stage; regulators need mechanisms to verify whether orders and corrective measures have actually been implemented.

Dr. Olumide Babalola

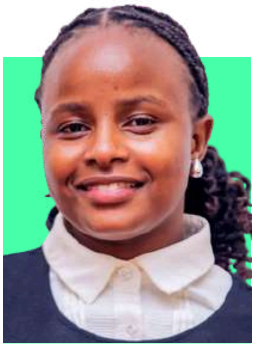
Founder, Data Privacy Lawyers' Association of Nigeria

Dr. Babalola examined the evolving jurisprudence of privacy and data protection in Africa, emphasizing that African courts and regulators needed to move beyond traditional understandings of privacy and develop legal principles capable of addressing emerging digital harms. Drawing from Nigerian litigation and comparative African experiences, he highlighted the importance of developing locally grounded jurisprudence, particularly in areas such as image rights, deepfakes, platform liability, sensitive data and cross-border data transfers.

Key pointers from Dr. Babalola's presentation:

- Privacy should not be understood only as protection against intrusion. Other dimensions include image rights, publication of embarrassing private facts and publicity in a false light.
- Image rights can constitute a privacy interest, even where traditional intellectual property law may not provide adequate protection.
- African courts are increasingly developing jurisprudence capable of addressing new forms of digital harm rather than relying exclusively on traditional legal causes of action. He pointed out that litigation involving a deepfake video, where an individual's image and voice were manipulated to falsely suggest that he had been healed of a terminal illness. The case demonstrated how emerging technologies can create privacy harms that traditional legal categories may not adequately capture.
- The development of privacy jurisprudence requires research-driven litigation. Lawyers and courts should not rely solely on residual or outdated knowledge when dealing with rapidly developing areas of technology law.
- Emerging issues such as platform regulation and platform liability require African lawyers and courts to examine their own domestic legal frameworks rather than assuming that global platforms are automatically protected by intermediary status.
- African jurisdictions should examine whether their existing laws adequately address the responsibilities of digital platforms and intermediaries.
- Imported data protection concepts require contextual adaptation. Concepts such as controllers, processors, processing and sensitive data were largely introduced through foreign regulatory models, but their application must reflect African realities.

- African definitions of sensitive personal data may need to reflect cultural realities. He noted that information considered particularly sensitive in African societies may differ from what is prioritised in Western legal systems.
- Financial information was highlighted as an example of data whose sensitivity may require greater recognition within African data protection frameworks.
- African countries should not assume that foreign judicial authorities provide automatic answers to local data protection questions. Foreign decisions may be persuasive, but courts must ultimately interpret and apply the law according to their own jurisdictions and contexts.
- The growth of local data protection decisions is essential to developing a body of African jurisprudence that lawyers, regulators and courts can rely upon.
- There is a need for Africa-wide jurisprudence and greater judicial dialogue so that courts across the continent can learn from each other's decisions and develop more coherent approaches to emerging digital issues.
- Courts will continue to encounter novel arguments as technology develops. The speaker illustrated this through disputes over whether photographs constitute personal data, demonstrating the need for clearer jurisprudence.
- Cross-border data transfers require greater clarity. African laws differ in their approaches, and uncertainty remains regarding what activities should legally constitute a cross-border transfer.
- African legislators and regulators should deliberately clarify key legal terminology, rather than continuing to rely on inherited definitions that may not adequately address modern digital transactions.



Irene Makau

The Oversight Lab Africa

Irene Makau examined the challenges of data protection, privacy, freedom of expression and online safety in Kenya, particularly in relation to technology platforms and the people who depend on them. She highlighted the difficulty of balancing the social, cultural and economic benefits that digital platforms provide to users and content creators with the need to protect privacy, prevent online harms and ensure that platforms comply with national data protection laws.

Key pointers from Irene's presentation:

- Platforms must comply with national data protection laws. Technology companies operating in African markets should ensure that their collection and processing of personal data complies with the applicable domestic legal framework.
- Data collection should be necessary and proportionate. Platforms should ensure that the information collected from users is necessary for the purposes for which it is processed.
- Online safety is an important part of data governance. Protection should extend to issues such as harassment, violence and other online harms, particularly where vulnerable users and content creators are affected.
- African realities must be reflected in platform governance. Technology platforms and their content moderation and data practices should take account of African languages, cultures and local contexts.
- Jurisdiction remains a major challenge. Many major technology companies are headquartered outside Africa, making it difficult for African regulators and affected individuals to obtain information, enforce decisions and secure effective remedies.
- Local representation can strengthen enforcement. Where technology companies rely on local entities or representatives, regulators may have greater practical ability to engage with them and address violations.
- Even where legal protections exist, limited public understanding and complicated procedures can prevent affected individuals from effectively seeking remedies.
- Regulators should become more proactive. Irene cautioned against waiting until violations become widespread before regulatory intervention begins.
- Algorithms and digital systems should be auditable. Regulators need sufficient access to information to understand how systems operate and how they collect and process personal data.
- African regulators should cooperate across borders. The cross-border nature of technology companies means that enforcement should not remain isolated within individual jurisdictions.

Jasper Twesige
Cavenbridge Advocates

As moderator, Mr. Twesige brought together the discussion on data protection, privacy and Big Tech accountability in Africa, highlighting the practical challenges faced by regulators and courts in addressing global technology companies. The session emphasized the need for proactive enforcement, stronger regional cooperation, algorithmic accountability and locally grounded African jurisprudence to address emerging digital harms.

The discussion ultimately underscored that effective digital accountability requires more than legislation. It requires capable institutions, informed regulators, accessible remedies and courts willing to develop the law alongside technological change.

SESSION RECORDING


BTA
SUMMIT
THE AFRIC
ACCOUNT
SUMMIT
Kampala, U
30-31 JULY
DELEGATE

#AdLegal

SESSION TWO | REPORT

Regulatory Overlaps and Turf Wars: When Too Many Agencies Regulate the Same Platform

About the Session:

The session examined the growing challenge of overlapping regulatory mandates in Africa's digital economy, where a single platform or digital service may simultaneously fall under data protection, competition, communications, financial services, consumer protection and other sector-specific regulators. Drawing on experiences from Uganda, South Africa and Nigeria, the session explored how fragmented legal and institutional frameworks can create jurisdictional uncertainty, duplicated compliance obligations and difficulties in coordinating investigations and enforcement.

The discussion highlighted Uganda's experience in coordinating data protection enforcement with sector regulators, particularly in relation to digital money lenders and telecommunications companies, while South Africa's approach demonstrated the value of structured cooperation between regulatory institutions. The private sector perspective further highlighted the burden created when companies face different reporting standards, overlapping requirements and multiple enforcement actions across African jurisdictions. The session ultimately emphasized the need for regulatory cooperation, harmonised approaches, information sharing and clearer institutional mandates to ensure that African regulators can effectively hold Big Tech and other digital platforms accountable without creating unnecessary regulatory fragmentation.

Expert Speakers:

Othieno Davis

Manager Compliance & Investigations, Personal Data Protection Office, Uganda

Speaker

Collin Dimakatso Mashile

Chief Director, Communications and Digital Technologies Department of the Republic of South Africa

Speaker

Ifeanyi E. Okonkwo,

Stillwaters Law Firm, Nigeria

Speaker

Joel Namugera

DPO East Africa

Session Chair

Speaker Submissions

Othieno Davis

Manager
Compliance &
Investigations,
Personal Data
Protection Office,
Uganda

Mr. Othieno examined the challenges of jurisdictional overlap and regulatory coordination in Uganda's digital economy, drawing on the Personal Data Protection Office's experience dealing with digital money lenders, telecommunications companies and other regulated entities. He emphasized that data protection cuts across multiple sectors, making cooperation between the PDPO and sector regulators essential to effective enforcement.

Key pointers from Mr. Othieno's presentation:

- Jurisdictional overlap often arose from Uganda's fragmented regulatory framework, where different laws assigned responsibilities to multiple sector regulators.
- Digital money lenders accounted for approximately 40% of the PDPO's case portfolio, with unlawful disclosure and processing of personal data identified as particularly common violations.
- The PDPO had worked with sector regulators such as UMRA in addressing data protection concerns involving digital money lenders.
- Complaints involving telecommunications companies had required cooperation between the PDPO and the Uganda Communications Commission.
- The PDPO's mandate cut across sectors because data protection obligations were embedded in almost every area of economic and public activity.

- Regulatory overlap could become particularly complex where a sector regulator was itself subject to data protection obligations and compliance requirements.
- Davis emphasized the importance of inter-regulatory collaboration rather than regulators operating in isolation.
- The PDPO had established formal collaborative frameworks with several sector regulators, including the National Lotteries and Gaming Regulatory Board, Insurance Regulatory Authority and Uganda Communications Commission.
- The Office intended to expand these Memoranda of Understanding and collaborative arrangements to additional regulators.
- Effective digital regulation required regulators to recognise that emerging technology issues often cross traditional sectoral boundaries.
- Big Tech, digital lending, telecommunications and other digital services require coordinated regulatory responses, particularly where data protection intersects with financial, communications, competition or consumer protection regulation.

Core message: Effective data protection enforcement in Uganda required regulators to move beyond institutional boundaries and build structured cooperation, information sharing and coordinated enforcement mechanisms across the digital economy.

Collin Dimakatso Mashile

Chief Director, Communications and Digital Technologies Department of the Republic of South Africa

Mr. Dimakatso examined the importance of regulatory coordination in South Africa's digital and communications ecosystem, emphasizing the need for competition, information regulation and other relevant authorities to work together as digital markets increasingly cut across traditional regulatory boundaries.

Key pointers from Mr. Dimakatso's presentation:

- South Africa had developed mechanisms for coordination among economic and digital regulators to address issues that fall across different regulatory mandates.
- The emergence of digital platforms and online harms had made cooperation between regulators increasingly important.

- Regulatory coordination helped prevent fragmented or conflicting approaches when different regulators were dealing with the same digital market or operator.
- Regulators needed to engage collectively when a particular issue involved competition, communications, broadcasting, information regulation or other overlapping areas.
- Coordination allowed regulators to consider the views of different institutions while ensuring that each regulator's position remained informed by its respective legal mandate and expertise.
- The experience demonstrated the importance of senior-level institutional coordination in managing complex digital regulatory questions.
- As technology and Big Tech business models continued to evolve, regulators needed mechanisms that could respond collectively to emerging digital challenges rather than operating within isolated regulatory silos.

Core message: Effective digital governance required strong institutional coordination and regulatory coherence, particularly where the activities of technology companies simultaneously raised competition, communications, data and broader digital policy concerns.

Ifeanyi E. Okonkwo,

Stillwaters Law Firm, Nigeria

Mr. Okonkwo examined the regulatory and compliance burden facing Big Tech and other digital companies operating across multiple African jurisdictions, highlighting the difficulties created by duplicated reporting requirements, divergent regulatory expectations and fragmented enforcement approaches.

Key pointers from Mr. Okonkwo's presentation:

- Digital companies operating across Africa faced duplicated compliance and reporting requirements from different regulators and jurisdictions.
- Different countries and regulatory authorities often imposed divergent expectations and compliance standards, creating uncertainty for businesses.
- A single incident, such as a data or cybersecurity breach, could expose a company to investigations, penalties and regulatory action in several African countries simultaneously.

- Companies could therefore face multiple fines for the same underlying incident, including potential enforcement from regulators in Kenya, Ghana, South Africa and other jurisdictions.
- Beyond financial penalties, regulatory investigations created significant reputational risks, particularly for major international brands.
- Fragmented regulatory requirements also created operational distractions, as companies had to respond separately to regulators and compliance obligations in each country.
- Conflicting or overlapping requirements could increase the cost of compliance, particularly for companies operating across several African markets.
- The discussion highlighted the need for greater regulatory coordination and harmonisation across African jurisdictions.
- More consistent regulatory standards could reduce unnecessary duplication while allowing regulators to maintain effective oversight of digital businesses.

Core message: Africa's fragmented regulatory environment can create significant compliance and enforcement burdens for digital companies. Greater regulatory convergence, cooperation and coordination would help address these challenges while strengthening accountability across the continent.

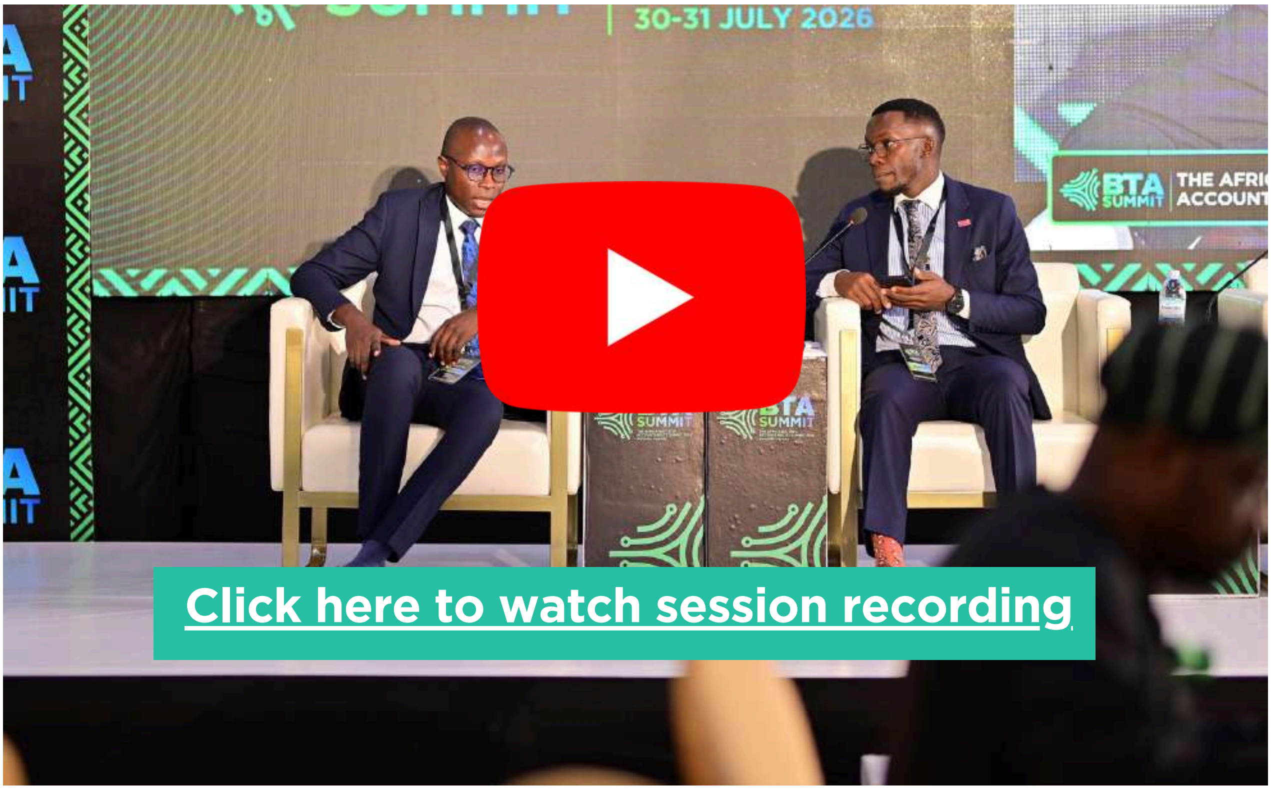
Joel Namugera

DPO East Africa

As session chair, Mr. Namugera brought together perspectives on the challenges created by regulatory overlap in Africa's rapidly evolving digital economy. The discussion highlighted how data protection, competition, communications, financial regulation and other regulatory mandates increasingly intersect, creating the need for stronger coordination among institutions.

The session demonstrated that fragmented regulatory frameworks can create duplicated compliance obligations, jurisdictional uncertainty and multiple enforcement exposures for digital businesses operating across African markets. Speakers highlighted practical experiences from Uganda and South Africa, as well as the private sector perspective from Nigeria, emphasizing the value of formal cooperation mechanisms, information sharing and regulatory convergence.

SESSION RECORDING



[Click here to watch session recording]

#AdLegal

SESSION THREE | REPORT

Who Shapes Africa's Digital Policy? Big Tech, Policy Entrepreneurship and the Future of Africa's Tech Regulation

About the Session:

The session was hosted in collaboration with the **Centre for Law, Policy and Innovation Initiative (CeLPII)** and it examined how digital policy agendas are shaped in Africa and the growing influence of Big Tech and other external policy actors in the development of regulatory frameworks for AI, digital platforms, data protection and emerging technologies. It explored how policy ideas, technical expertise and regulatory models are introduced, adapted and contested within African policymaking processes, while considering both the benefits and risks of engagement with technology companies, international organisations, development partners, academia and civil society.

Across Africa, governments are developing new legal and policy frameworks to govern artificial intelligence, digital platforms, data protection, cybersecurity and other emerging technologies. Over the past decade, the continent has witnessed significant growth in digital regulation, with most African countries now having enacted or in the process of enacting data protection legislation. Several countries, including Nigeria, Rwanda and Kenya, have also published or are developing national AI strategies and considering broader approaches to AI governance. These developments reflect a growing recognition that digital technologies require governance frameworks capable of protecting citizens, promoting innovation and supporting economic transformation.

Expert Speakers:

Dr. Melody Musoni
Policy Analyst, ECDPM

Speaker

Dr. Mark Gaffley
Director Legal and Operations, Global Center on AI Governance

Speaker

Bonaventure Saturday,
Research manager, Pollicy

Speaker

Janice Celine Nantumbwe,
Head of Policy, CeLPII

Speaker

Zaina Nakyagaba
KTA Advocates

Session Chair

Session Convenors:

CENTRE FOR LAW, POLICY, AND INNOVATION INITIATIVE

#AdLegal

Speaker Submissions

Dr. Melody Musoni
Policy Analyst, ECDPM

Dr. Melody examined the relationship between African digital policy, digital sovereignty and external influence, emphasizing that Africa's approach to emerging technologies had historically been shaped by efforts to close the digital divide, expand infrastructure and develop digital skills. She argued that as AI and other technologies continued to reshape economies, Africa needed to move beyond regulatory responses and build greater agency across the entire technology ecosystem.

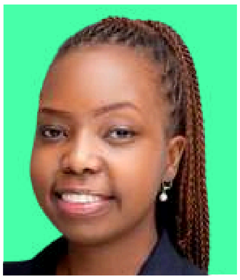
Key pointers from Dr. Melody's presentation:

- African digital policy had historically focused on closing the digital divide, expanding infrastructure, improving connectivity and developing digital skills.
- The rise of AI had expanded the policy conversation, requiring African countries to consider how emerging technologies were changing business, work and social interaction.
- Digital sovereignty was presented as a response to digital colonialism, particularly concerns about the exploitation of African data and labour.

- Africa's digital policy agenda has continued to be influenced by external actors, particularly the European Union and international development agencies. The EU's regulatory influence has been illustrated through the impact of European data protection standards on African data protection regimes.
- Dr. Musoni cautioned against allowing externally driven priorities to displace Africa's own development agenda, particularly in relation to digital public infrastructure and digital ID.
- Digital sovereignty was described as being more than regulatory authority. It also required control over infrastructure, markets, technology value chains, data and the ability to create economic value from African resources.
- Africa therefore needs to reconsider approaches such as strict data localisation, focusing instead on how data could generate value within African economies while supporting appropriate cross-border data flows.
- The continent should invest in African-owned technology businesses, particularly those capable of developing infrastructure and providing ICT services.
- Partnerships between Big Tech and African companies could provide a gradual pathway towards reducing excessive dependence on foreign technology providers.
- African countries needed to ensure that AI systems and data infrastructure reflected African languages, cultures, knowledge systems and environments, rather than relying entirely on technologies developed around external realities.
- Digital sovereignty required investment across the entire technology stack, including infrastructure, energy, skills, data, businesses and regulatory frameworks.
- Africa needs to prepare young people for the future of work by investing in AI and digital skills.
- Regional cooperation was critical. African countries should avoid developing completely isolated digital systems and instead explore shared infrastructure, including regional data centres and emerging concepts such as data embassies.

Core Takeaway

Dr. Musoni's central message was that African digital sovereignty could not be achieved through regulation alone. It required Africa to build greater ownership and influence across infrastructure, technology markets, skills, data, AI value chains and local businesses, while strengthening regional cooperation and ensuring that the continent's digital agenda was shaped by African priorities and realities.



Janice Celine Nantumbwe, Head of Policy, CeLPII

Janice examined the challenge of developing technology regulation that is both responsive to emerging risks and grounded in African realities. She acknowledged the practical pressure on policymakers to regulate quickly, which often makes established frameworks from the EU and United States attractive starting points. However, she cautioned against adopting such frameworks wholesale, emphasizing that laws and policies must be adapted to local institutional capacity, social realities and regulatory needs.

Key pointers from Janice's presentation:

- Policymakers need to exercise regulatory discernment. Rather than simply asking what another jurisdiction has done, African policymakers should determine which elements of foreign frameworks can realistically work within their own jurisdictions.
- Policy conversations should include policymakers. Discussions involving lawyers, technologists, civil society, academia and industry should reach policymakers so that expertise generated outside government can inform actual legislative and regulatory processes.
- Government should not develop technology policy in isolation. The private sector often encounters emerging technological risks in real time and can therefore provide regulators with practical knowledge about how new technologies operate and where potential harms may arise.
- Regulatory independence remains essential. While governments should learn from industry, they must maintain sufficient independence to avoid regulatory capture and ensure that public interest considerations remain central.
- Public-private collaboration can improve regulation. Janice pointed to the NIST framework as an example of collaboration between government and industry in identifying technological risks and developing appropriate responses.

- Industry self-regulation can complement government regulation. Technology companies can test internal safeguards and identify risks through responsible experimentation, although such self-regulation should not replace appropriate government oversight.
- Governments should establish regulatory guardrails. Regulators should create boundaries within which emerging technologies can be tested and developed, rather than attempting to anticipate and prohibit every possible technological development.
- Regulation should learn from technological experimentation. Where companies identify new risks through testing and deployment, those lessons should be communicated to policymakers and used to improve future regulatory frameworks.
- The ultimate approach should be a combination of global learning and African adaptation. Africa does not need to choose between creating regulation entirely from scratch and copying foreign models; it can draw from international experience while developing a context-specific regulatory mosaic.

Core message: Effective technology regulation requires local context, institutional capacity, regulatory independence and meaningful government-industry collaboration. International frameworks should inform African regulation, but should not substitute for African policy thinking and decision-making.

Bonaventure Saturday,
Research manager, Pollicy

Mr. Bonaventure Saturday focused on the need for Africa to build the technical, institutional and societal capacity required to understand, govern and regulate AI effectively. He argued that the development of AI regulation should not come before the development of the expertise and evidence needed to make that regulation meaningful.

This included investing in AI evaluation laboratories, developing technical expertise across government and the judiciary, strengthening AI education and increasing public awareness. He further emphasized that African countries should domesticate international AI frameworks rather than replicate them, developing laws that reflect African realities and community structures.

Key pointers from Mr. Bonaventure's presentation:

- African countries should develop dedicated labs to test AI systems, understand how they operate and identify potential risks before those systems become widely deployed.
- Bonaventure highlighted the significant shortage of AI expertise in Africa, emphasizing the need for deliberate investment in developing local technical talent.
- Judges and courts need sufficient understanding of AI to effectively handle disputes involving automated decision-making, algorithmic systems, discrimination, data and AI-related harms.
- European and other international AI laws can provide principles and starting points, but African countries should develop laws based on their own realities rather than simply reproducing foreign frameworks.
- Governments should create controlled environments where emerging technologies can be tested and studied to generate African evidence on AI risks and impacts.
- Bonaventure referred to Uganda's Ministry of ICT's innovation facilities, including the ICT Hub, as an example of how controlled environments can support technology experimentation and evidence generation.
- Incorporate the principle of Ubuntu. AI governance should recognize the African reality of community and collective life. Rather than focusing exclusively on individual protection, regulatory frameworks should also consider harms and protections at the community level.
- Adoption of a bottom-up regulatory approach. AI laws should be informed by the experiences of people at the local level rather than being developed exclusively from the perspective of policymakers and institutions.
- Policymakers should engage communities directly to understand how AI systems are affecting people in practice and incorporate those experiences into regulatory design.

Core message:

Africa should not simply import AI laws developed elsewhere. It should build the expertise, evidence, institutions and public awareness necessary to develop and enforce AI governance frameworks that are technically informed, community-conscious and grounded in African realities.

Dr. Mark Gaffley
Director Legal and Operations, Global Center on AI Governance

Dr. Gaffley examined how African countries can strengthen their digital sovereignty and develop technology and AI governance frameworks that are inclusive, locally grounded and responsive to African realities.

He highlighted the risk of digital colonialism and continued North–South dependency, arguing that Africa should strengthen local talent, evidence generation and South–South cooperation rather than relying predominantly on externally developed approaches.

Key pointers from Dr. Gaffley's presentation:

- Africa should guard against digital colonialism. Data, technology and digital infrastructure should not reinforce historical South-North relationships or create new forms of extractive dependence.
- African AI strategies should be built around inclusion. Nigeria was highlighted as an example of a country that mapped Nigerian AI talent and academic expertise globally and brought researchers, startups, civil society and other stakeholders together to develop its national AI strategy.
- African countries should actively mobilise their diaspora talent. Identifying African professionals working around the world can help countries access expertise that can contribute to national technology and AI strategies.
- Policy development should involve the right people. Governments should ensure that innovators, academics, startups, civil society, technical experts and policymakers participate meaningfully in shaping digital regulation.
- South-South cooperation can strengthen African policymaking. African policymakers should learn from one another and share experiences on domestic AI strategies rather than relying exclusively on principles developed by institutions in the Global North.
- Peer learning between African countries is important. Platforms bringing together policymakers from countries such as Ghana, South Africa, Kenya, Rwanda and Uganda can facilitate practical exchange of experiences and approaches to AI governance.

- Not every technological development requires new legislation. Governments should first assess whether existing consumer protection, data protection, competition, labour and other laws can already address the risks created by AI and digital technologies.
- Over-regulation can unintentionally disadvantage African startups. Additional regulatory requirements may be easier for large technology companies to absorb because they have established legal, compliance and technical teams, while smaller innovators may struggle with the additional burden.
- Regulation should remain proportionate and evidence-based. Policymakers should identify the actual regulatory gap before creating new laws and avoid introducing rules simply because a technology is new.
- Participatory policymaking is essential. Local innovators and businesses should have a voice in determining what should be regulated and how regulation should operate in practice.
- Governments should be alert to vendor lock-in. Public procurement of digital technologies can create long-term dependence on particular foreign technology providers, limiting Africa's ability to control its own digital infrastructure.
- Investment incentives can support local digital capacity. Tax incentives and other mechanisms could encourage experienced investors to invest in African startups while transferring knowledge, expertise and compliance capabilities to emerging businesses.
- Africa's digital future depends heavily on retaining talent. The continent needs stronger incentives to prevent the continued loss of skilled technology professionals through brain drain.
- Education and skills development should be a long-term policy priority. Investments in local education, digital skills, AI training and EdTech could significantly strengthen Africa's ability to develop and govern its own technologies.
- Technology policy should create local opportunities. Policies aimed at attracting digital professionals should go beyond bringing foreign workers into Africa and should encourage genuine local skills development and knowledge transfer.

Core message: Africa's ability to shape its digital future will depend not only on the laws it adopts, but on whether it develops home-grown expertise, retains talent, builds inclusive institutions and creates policies that reflect African realities while enabling local innovation.

Zaina Nakyagaba
KTA Advocates

As session chair, Ms. Zaina Nakyagaba brought together the different perspectives from the panel and highlighted the importance of developing African-led approaches to AI governance and regulation.

The discussion emphasized that while international frameworks can provide useful starting points, African countries need to adapt them to their own realities, strengthen institutional and technical capacity, invest in local evidence and AI research, and ensure meaningful participation of policymakers, industry, civil society, academia and communities.

SESSION RECORDING

#AdLegal

SESSION FOUR | REPORT

Advocacy as an Enforcement Trigger: How Civil Society and Public Interest Litigation Drive Big Tech Data Protection Accountability in Africa

About the Session:

The session examined the growing role of civil society, public interest organizations and affected communities in driving Big Tech data protection accountability in Africa. It explored how advocacy, public interest litigation, regulatory engagement and strategic interventions could trigger greater accountability where dominant technology platforms' practices raised concerns around privacy, data protection, consumer rights and the broader public interest.

The discussion highlighted the importance of civil society as an independent accountability actor, particularly where regulatory institutions may face capacity, resource or enforcement constraints.

The session considered how African civil society organizations could use litigation, research, public advocacy and engagement with regulators to identify emerging harms, influence enforcement priorities and ensure that the rights and interests of African users were reflected in the governance of digital platforms and data-driven technologies.

The discussion also examined the need for stronger collaboration between civil society, regulators, courts, media organizations and affected communities to ensure that data protection frameworks translate into meaningful accountability and effective remedies for African users.

Expert Speakers:

Patricia Ainembabazi

Policy & Advocacy Officer - CIPESA

Speaker

Raymond Amumpaire

Complainant in Google Data Privacy Case in Uganda

Speaker

Dr. Faith Amarachi Okpara

Vice President, DPLAN

Speaker

Yasmin Ahmed

Director of Programs, FemTech Law Initiative

Session Chair

Speaker Submissions

Patricia Ainembabazi

Policy & Advocacy Officer - CIPESA

Patricia highlighted the role of evidence-based advocacy, capacity building and public engagement in strengthening Big Tech accountability and digital rights protection in Africa. She explained that civil society's role complemented litigation and regulation by documenting digital harms, conducting research, building the capacity of judges and policymakers, and creating platforms for direct engagement with technology companies.

Key pointers from Patricia's presentation:

- Civil society complements, rather than replaces, regulators and courts. Advocacy was presented as a means of supporting effective regulation and accountability.
- Evidence collection is central to effective advocacy. Documentation and research provide the factual basis for litigation, policy reform and regulatory intervention.

- Capacity building strengthens the entire accountability chain. CIPESA has worked with judges, lawyers, parliamentarians and policymakers on digital rights, data protection and emerging technology issues.
- Judicial capacity is particularly important. Training judges across East Africa, SADC and other parts of the continent helps courts understand increasingly complex digital rights and technology disputes.
- Africa's fragmented regulatory frameworks remain a major challenge. Different national data protection regimes make it harder to address cross-border digital harms consistently.
- Greater harmonisation of African data protection rules is needed, particularly for cross-border data disputes.
- The African Union Data Protection Framework (AUDPF) provides a foundation for greater continental consistency, but its non-binding nature limits its effectiveness.
- Regional approaches can produce stronger outcomes than isolated national action. She pointed to the EU's common USB-C charging standard as an example of how coordinated advocacy and policymaking can influence Big Tech and technology markets.
- Parliamentarians require continuous technical capacity building, particularly because parliamentary committees and memberships change over time.
- Institutional memory matters: experienced advocates and policymakers can help new legislators understand previous policy discussions and emerging technology trends.
- Sustained advocacy requires an enabling environment and resources. Civil society organisations need adequate support to maintain long-term engagement with governments, regulators and technology companies.
- Big Tech engagement should be used strategically: dialogue with company representatives provides an opportunity to obtain explanations and commitments, while civil society must continue to perform its independent watchdog role.
- **Core message:** Effective Big Tech accountability in Africa requires a connected ecosystem of research, advocacy, litigation, judicial and legislative capacity building, regional harmonisation and sustained engagement with technology companies.

Raymond Amumpaire

Complainant in Google Data Privacy Case in Uganda

Raymond presented the Google data privacy case in Uganda as an example of how public interest litigation and civil society advocacy could be used to test the accountability of Big Tech under national law. He explained that the complaint challenged Google's compliance with Uganda's data protection framework, including its registration obligations and cross-border data transfers, while also raising broader questions of digital sovereignty, institutional accountability, human rights and the unchecked concentration of data and technological power.

Key pointers from Raymond's presentation:

- The case was framed not only as a data protection matter, but also as a question of digital sovereignty and the accountability of powerful technology companies.
- The litigation tested the effectiveness of Uganda's Personal Data Protection Office (PDPO) as the institution responsible for enforcing the data protection framework.
- The case demonstrated that citizens can use existing legal frameworks to challenge the conduct of Big Tech, even where the companies are headquartered outside Africa.
- Weak penalties can undermine accountability. He argued that small financial sanctions do not create a meaningful deterrent for global technology companies whose revenues vastly exceed the value of such penalties.
- Effective remedies matter. He pointed out that regulators need sufficient authority to impose meaningful sanctions and remedies without requiring complainants to pursue additional proceedings before other institutions.
- Regulatory capacity is critical. He highlighted the significant disparity between the resources available to African regulators and those available to global technology companies.
- The case revealed challenges around delays and regulatory processes, particularly where regulators are dealing with highly resourced Big Tech companies.
- Public interest litigation alone is insufficient. It needs to be supported by research, public education, advocacy and sustained engagement with policymakers.

- Legislative reform is necessary to ensure that Uganda's data protection laws reflect the realities of Big Tech and provide regulators with adequate enforcement powers.
- Lobbying by Big Tech requires scrutiny. Amumpaire highlighted the importance of monitoring how technology companies influence digital, AI and data-related policymaking.
- **Core message:** Big Tech accountability requires more than having laws on the books; African countries need meaningful sanctions, adequately resourced regulators, effective remedies, public interest litigation, research and sustained advocacy to ensure that global technology companies comply with national law.

Dr. Faith Amarachi Okpara

Vice President, DPLAN

Dr. Amarachi examined the current state of Big Tech data protection accountability in Africa, using Nigeria as a leading example of both regulatory progress and persistent enforcement gaps. She highlighted the landmark FCCPC/NDPC investigation into Meta and WhatsApp, the role of courts and civil society in challenging enforcement outcomes, and the continuing need for stronger institutional capacity, transparency and regional cooperation.

Key pointers from Dr. Amarachi's presentation:

- Africa has moved beyond having data protection laws only on paper. Regulators, courts and civil society are increasingly using those laws to demand accountability from major technology companies.
- Nigeria's Meta/WhatsApp investigation demonstrated that African regulators can investigate Big Tech, impose significant penalties and secure corrective measures.
- The US$220 million Meta penalty and subsequent enforcement actions demonstrated that Big Tech companies can face meaningful consequences under African law.
- However, fines alone do not guarantee lasting accountability. The form of enforcement—binding decisions versus negotiated settlements—can significantly affect deterrence and the durability of regulatory outcomes.

- DPLAN challenged the legality and public-interest implications of the Meta settlement, raising questions about regulatory authority, representation of affected data subjects and transparency in settlements.
- Civil society must remain an independent accountability mechanism, ensuring that regulatory decisions remain subject to public scrutiny even after enforcement proceedings conclude.
- Strong legislation requires effective institutions, clear procedures, technical expertise and adequate operational capacity to translate legal rights into practical protection.
- Regulatory delays are a serious concern, particularly because technology markets and data-driven business models develop much faster than regulatory processes.
- The experience of Nigeria, Kenya, South Africa and Uganda demonstrated that regulators, courts and civil society were increasingly active, but accountability could not depend on exceptional landmark cases alone.
- Africa needs a shared reference framework for digital accountability, particularly around jurisdiction, cross-border data transfers, lawful processing, consent and regulatory cooperation.
- Information sharing between African regulators can prevent duplication and allow authorities to build on investigations and precedents developed elsewhere on the continent.
- Regional cooperation should extend beyond regulators to include civil society organizations and professional networks, which can identify harms, gather evidence and initiate public-interest interventions before formal regulatory action begins.
- The future of Big Tech accountability was framed around three interconnected actors: regional bodies, courts and tribunals, and civil society.
- **Core message:** Africa's challenge is no longer simply creating data protection laws, but building a connected enforcement ecosystem in which regulators have authority and capacity, courts provide effective oversight, and civil society maintains sustained public accountability.

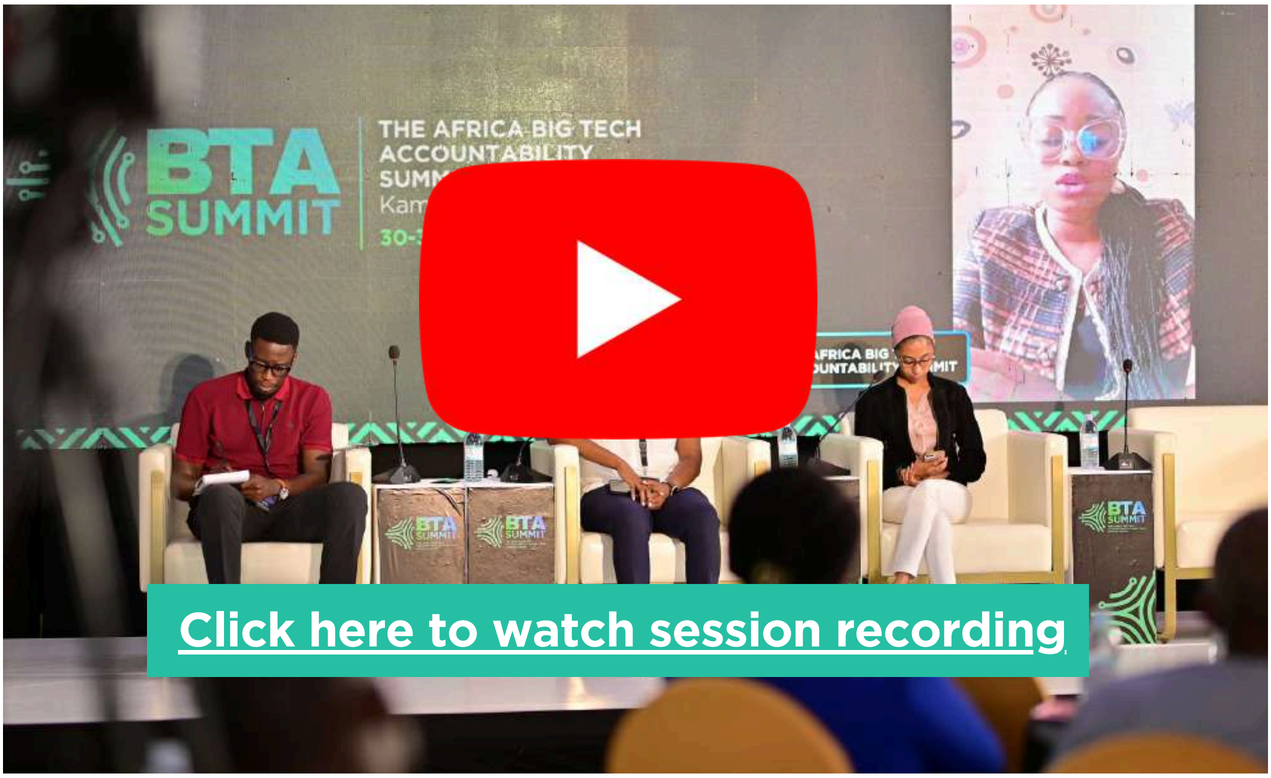
Yasmin Ahmed

Director of Programs, FemTech Law Initiative

As **Session Chair**, Yasmin brought together the panel's perspectives on the evolving role of civil society and public interest advocacy in driving Big Tech data protection accountability in Africa. The discussion demonstrated that meaningful accountability could not depend on regulators alone. Civil society plays a critical role in documenting harms, initiating complaints and litigation, building the capacity of judges and policymakers, and maintaining public scrutiny of how technology companies operate across African jurisdictions.

The session also highlighted the need for stronger regional cooperation, effective regulatory institutions, meaningful remedies and greater harmonisation of data protection frameworks. She wrapped the session up by documenting that Africa needed to move beyond laws on paper towards practical and lasting protection of African users, with civil society serving not only as an enforcement trigger but as a permanent accountability partner in the digital governance ecosystem.

SESSION RECORDING



#AdLegal

SESSION FIVE | REPORT

The Role of Data Privacy Lawyers' Associations in Shaping Data Protection Practice and Enforcement in Africa

About the Session:

The session brought together the Forum for Data Protection Practitioners Uganda (FDPPUG) and the Data Privacy Lawyers Association of Nigeria (DPLAN) to examine The Role of Data Privacy Lawyers' Associations in Shaping Data Protection Practice and Enforcement in Africa.

The session explored how professional associations can strengthen data protection practice by building practitioner capacity, promoting ethical standards, engaging regulators, contributing to legislative and regulatory development, undertaking advocacy and supporting strategic litigation. Speakers reflected on the experiences of the two associations and the importance of creating strong professional communities that can identify implementation gaps and develop appropriate responses through engagement, advocacy, research, advisory work and litigation.

The session ultimately demonstrated that effective Big Tech accountability requires a strong and organized professional community alongside capable regulators. By connecting practitioners across jurisdictions, contributing African perspectives to policy development, supporting enforcement and pursuing strategic interventions where necessary, data privacy lawyers' associations can play a critical role in shaping a more effective, locally grounded and accountable data protection ecosystem across Africa.

Expert Speakers:

Ivan Ojakol

Founder, Forum for Data Protection Practitioners Uganda (FDPPUG)

Speaker

Dr. Olumide Babalola

Founder, Data Privacy Lawyers Association of Nigeria (DPLAN)

Speaker

Bibitayo Ojo

Member, Data Privacy Lawyers Association of Nigeria (DPLAN)

Speaker

Daisy Bigabwa

Member, Forum for Data Protection Practitioners Uganda (FDPPUG)

Session Chair

Speaker Submissions

Ivan Ojakol

Founder, Forum for Data Protection Practitioners Uganda (FDPPUG)

Mr. Ojakol examined the implementation gap in data protection and privacy enforcement in Uganda, emphasizing the need for stronger collaboration among lawyers, cybersecurity professionals, technology experts and other practitioners. He highlighted the role of professional networks in strengthening privacy awareness, supporting strategic litigation and helping policymakers develop more effective and harmonised data protection frameworks across Africa.

Key pointers from Mr. Ojakol's presentation:

- Uganda had made progress in data protection enforcement, but a significant implementation gap remained.
- The Forum for Data Protection Practitioners Uganda was established to bring together lawyers, cybersecurity experts, IT professionals and other specialists to strengthen implementation of data protection principles.

- Unlike some other African jurisdictions, Uganda's PDPO faced limitations in imposing monetary penalties, with enforcement often taking the form of declarations and other regulatory measures.
- Strategic litigation had played an important role in advancing data protection accountability, with cases involving SafeBoda, Meta and other entities demonstrating the growing use of legal mechanisms to protect data subjects.
- Data protection should be treated as a cross-cutting issue, requiring expertise beyond the legal profession.
- Uganda needs to develop a stronger privacy culture, particularly because communal social practices can sometimes create different perceptions of what information should be considered private.
- The principle of privacy by design should become embedded in corporate decision-making and technology development.
- Data protection should receive greater attention at the corporate board level, similar to the growing prominence of ESG and sustainability considerations.
- The expansion of Big Tech and cross-border data flows created an opportunity for African professionals and institutions to ensure that the economic value generated from African data was retained and benefited African economies.
- African policymakers need support from competent local professionals when developing and harmonising data protection laws and policies.
- Professional associations could help bridge the gap between policy, regulation and practical implementation through research, publications, training, webinars and strategic litigation.
- FDPPUG had already undertaken initiatives including publications on data protection in public events and health data sharing, as well as capacity-building activities.
- The Forum intended to expand its activities through publications, events, strategic litigation and professional collaboration.
- Stronger networks are necessary because practitioners could achieve greater impact by working collectively rather than individually.
- Professional bodies should maintain a constructive relationship with regulators while also retaining the ability to hold regulators accountable where necessary.

Dr. Olumide Babalola

Founder, Data Privacy Lawyers Association of Nigeria (DPLAN)

Dr. Olumide emphasized the importance of building organic, cross-border professional networks to strengthen data protection practice and address implementation gaps across Africa. Drawing from the experience of the Nigerian data protection community, he explained that professional associations can grow gradually by demonstrating value, fostering solidarity and creating opportunities for learning. He also stressed that implementation gaps require different responses depending on their nature, ranging from advocacy and regulatory engagement to research, advisory work and strategic litigation.

Key pointers from Dr. Olumide's presentation:

- Dr. Babalola highlighted emerging partnerships between practitioners in Nigeria, Kenya, Uganda and Ghana, describing these connections as part of how broader professional movements develop across Africa. He emphasized that such partnerships should grow organically as practitioners recognize their value.
- He stressed the importance of community in Africa as a foundation for learning, professional development and solidarity. The participation of several Nigerian practitioners at the summit demonstrated how such networks can gradually expand.
- Reflecting on the Nigerian experience, he noted that the association had grown to more than 450 members despite being less than two years old. He viewed this growth as an important foundation for addressing implementation challenges over time.
- He argued that regulators should recognize the role of professional associations and consult them when developing regulations, legislation or amendments. Their practical experience can provide valuable input into policymaking.
- Professional associations should also watch the regulatory space, identifying areas where regulators have failed to issue necessary directives, clarify legal provisions or establish required institutional structures.

- Dr. Babalola explained that some implementation gaps can be addressed through direct engagement with regulators, including correspondence, advocacy and professional dialogue, without immediately resorting to litigation.
- Where engagement cannot resolve a legal or institutional gap, litigation can provide necessary clarification and establish authoritative interpretations of the law.
- He referred to litigation concerning the Nigerian regulator's attempt to register point-of-sale operators as an example. The case questioned whether the operators qualified as data controllers or processors, resulting in judicial clarification of the regulator's powers.
- He noted that the regulator itself welcomed the outcome because the judgment provided validation and clarity regarding its regulatory mandate. The case demonstrated that litigation can sometimes strengthen regulatory institutions rather than simply challenge them.
- Dr. Babalola emphasized that implementation problems can be addressed through advocacy, engagement, articles, advisory work or litigation, depending on the nature of the particular gap.
- He stressed the importance of first analysing the nature of the gap before selecting an intervention. This ensures that litigation is used where necessary while other issues are addressed through engagement, advocacy or technical support.

Core Takeaway

Dr. Babalola's central message was that closing Africa's data protection implementation gaps requires collective and strategic action. Professional associations can serve as important partners and watchdogs, while cross-border networks can strengthen solidarity and knowledge sharing. Ultimately, effective implementation requires a combination of engagement, advocacy, research, advisory support and strategic litigation, with the appropriate approach determined by the specific gap being addressed.

Bibitayo Ojo

Member,
Data Privacy
Lawyers Association
of Nigeria (DPLAN)

Mr. Bibitayo focused on the need for professional standards and ethical conduct among lawyers and other data protection practitioners who advise organisations.

He emphasized that existing professional obligations, particularly around confidentiality and the duty of care, should translate into the way practitioners handle privacy and data protection work. He also suggested that these principles should be embedded by design within professional practice so that ethical conduct becomes an inherent part of how practitioners interact with clients and industry.

Key pointers from Mr. Bibitayo's presentation:

- He emphasized the importance of developing standards that guide how privacy professionals interact with industry and clients, particularly where there is no specific framework or code governing such professional engagement.
- He pointed to existing legal professional rules of conduct, particularly obligations relating to confidentiality, as an important foundation for responsible privacy practice.
- He stressed that lawyers handling client information already have a professional duty to protect confidential information, and this obligation should naturally extend to their work as privacy and data protection practitioners.
- He highlighted provisions in professional codes that require practitioners to exercise care and responsible conduct, arguing that these principles should inform the conduct of privacy professionals.
- A central point was the need to embed ethical responsibilities by design, rather than treating professional conduct as something applied only after problems arise. Practitioners should be guided by professional standards throughout their work.

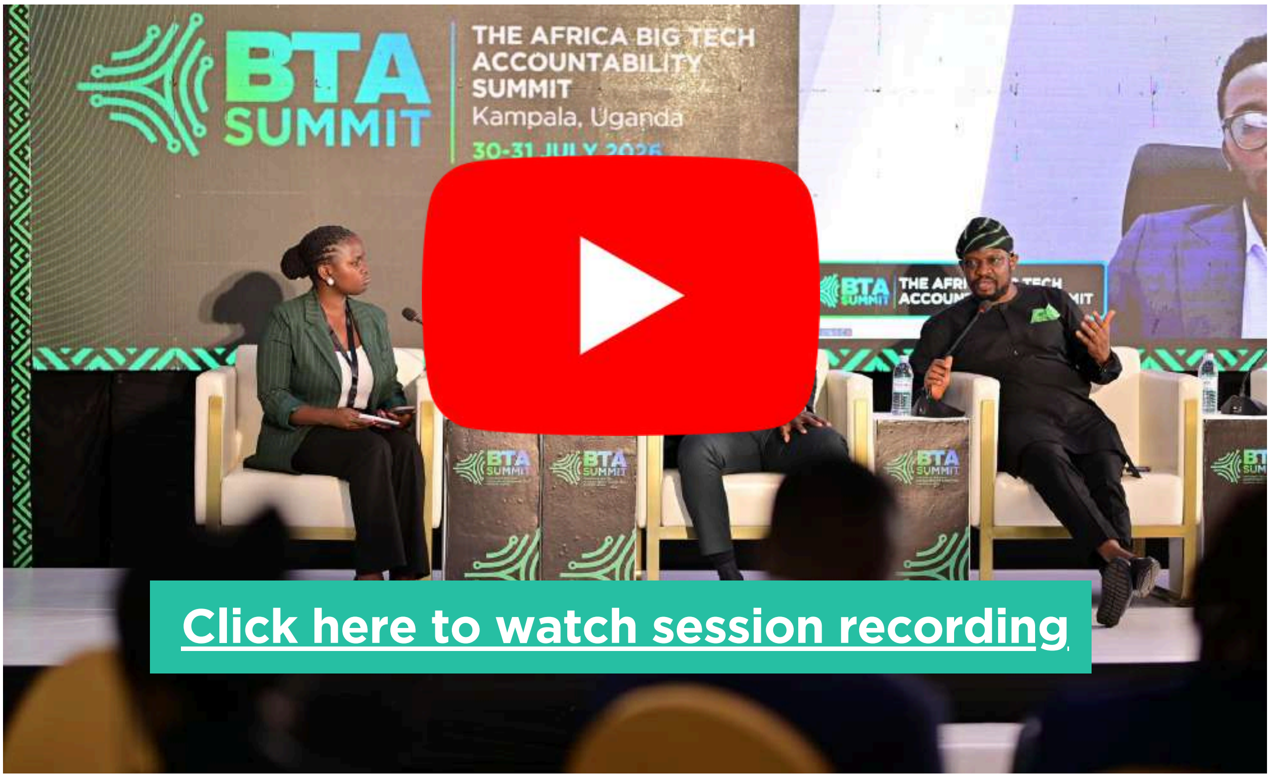
Daisy Bigabwa

Member,
Forum for Data Protection Practitioners Uganda (FDPPUG)

As session chair, Ms. Bigabwa brought together the discussion on strengthening professional standards, ethical practice and collaboration within Africa's data protection ecosystem. The session highlighted the importance of professional associations, regulatory engagement, cross-border partnerships and strategic litigation in addressing gaps in the implementation of data protection frameworks.

The discussion underscored that closing these gaps requires a multi-dimensional approach, combining advocacy, engagement, research, advisory support and litigation where necessary. It also emphasized the value of building strong professional communities across Africa that can support practitioners, contribute to policymaking and promote greater accountability in the data protection space.

SESSION RECORDING



Recommendations

Seven Pillars for Africa's Data Protection and Big Tech Accountability Agenda

Pillar 1

Recommendations:

ENFORCEMENT CAPACITY

African data protection laws should move beyond formal compliance towards effective enforcement capable of producing meaningful remedies against global technology companies.

Strategic Priorities:

- Strengthen the investigative, technical and enforcement capacity of Data Protection Authorities to investigate complex Big Tech data practices.
- Provide regulators with meaningful enforcement powers and remedies capable of creating an effective deterrent against multinational companies.
- Develop mechanisms for post-decision monitoring to ensure that regulatory orders result in actual changes to platform practices.
- Establish accelerated procedures for matters involving large-scale processing, sensitive data or significant risks to African data subjects.
- Require regulators to develop clear procedures for dealing with companies that operate in African markets but have no physical presence or assets within the jurisdiction.
- Ensure that enforcement focuses not only on fines but also on corrective measures, transparency, deletion, changes to processing practices, consent mechanisms and other remedies capable of protecting data subjects.

Pillar 2

Recommendations:

CLOSE THE JURISDICTION AND CROSS-BORDER ENFORCEMENT GAP

One of the strongest themes of the Summit was the **African Data Paradox.** Africans generate the data, while the companies, servers, contractual arrangements and corporate structures controlling that data are frequently located outside Africa. Extraterritorial legal powers therefore need to be matched with practical enforcement mechanisms.

Strategic Priorities:

- Develop clearer rules governing the extraterritorial application of African data protection laws to Big Tech platforms targeting or processing the data of African users.
- Require significant technology platforms operating in African markets to maintain an accessible local or regional representative for data protection and regulatory matters.
- Develop regional mechanisms for the recognition and enforcement of data protection decisions and judgments across African jurisdictions.

- Establish coordinated procedures for cross-border investigations and evidence gathering.
- Develop clearer and more consistent African rules on cross-border data transfers, including what constitutes a transfer and the safeguards required.
- Review contractual arrangements that effectively force African users to rely exclusively on foreign choice-of-law, jurisdiction and dispute-resolution mechanisms.
- Strengthen collective African enforcement so that a multinational platform cannot exploit differences between jurisdictions to avoid accountability.

Pillar 3

Recommendations:

DEVELOP AFRICAN JURISPRUDENCE FOR EMERGING PRIVACY HARMS

African courts and regulators should actively develop jurisprudence capable of addressing forms of digital harm that were not contemplated when many existing privacy laws were enacted. The Summit identified deepfakes, image rights, platform liability, sensitive data, photographs as personal data and emerging forms of digital processing as areas requiring clearer African legal principles.

Strategic Priorities:

- Establish stronger judicial capacity-building programmes on data protection, AI, algorithms, platform governance and emerging digital harms.
- Encourage research-driven strategic litigation capable of testing unresolved questions in African privacy law.
- Develop African jurisprudence on image rights, deepfakes, biometric data, profiling and algorithmic decision-making.
- Re-examine definitions of sensitive personal data to ensure that they reflect African social, cultural and economic realities.
- Develop jurisprudence addressing the responsibilities of digital platforms and intermediaries, rather than assuming that global platforms are automatically protected by intermediary status.
- Establish mechanisms for judicial dialogue across African jurisdictions, enabling courts to learn from decisions involving similar Big Tech and privacy issues.
- Develop African legal scholarship and databases documenting data protection decisions, regulatory orders and enforcement precedents across the continent.

Pillar 4

Recommendations:

BUILD A COORDINATED AFRICAN BIG TECH ACCOUNTABILITY FRAMEWORK

The Summit repeatedly demonstrated that Big Tech accountability cannot be achieved effectively through isolated national action. A single platform can simultaneously raise issues of data protection, competition, consumer protection, communications and online safety. Fragmented enforcement creates both accountability gaps and regulatory uncertainty.

Strategic Priorities:

- Establish stronger cooperation between African Data Protection Authorities on investigations involving multinational technology companies.
- Develop formal information-sharing mechanisms allowing regulators to share evidence, investigative findings, regulatory decisions and enforcement experience.
- Strengthen collaboration between data protection, competition, communications, consumer protection and other sector regulators.
- Develop joint or coordinated approaches to major Big Tech investigations where conduct affects users across several African jurisdictions.
- Strengthen the role of Regional Economic Communities and continental institutions in coordinating cross-border digital accountability.
- Work towards greater harmonisation of African data protection standards, particularly concerning jurisdiction, cross-border transfers, consent, lawful processing and platform accountability.
- Develop an African mechanism through which regulators can collectively engage Big Tech on continent-wide compliance expectations and remedies.

Pillar 5

Recommendations:

CIVIL SOCIETY AND PUBLIC INTEREST ACTORS

The Summit demonstrated that effective accountability cannot depend exclusively on regulators. Civil society, researchers, and affected communities can identify harms, generate evidence, initiate complaints and litigation, and maintain public scrutiny of Big Tech.

Strategic Priorities:

- Establish stronger mechanisms for data subjects and civil society organisations to submit evidence and complaints to Data Protection Authorities.
- Support public-interest organisations undertaking research and documentation of Big Tech data practices and digital harms.

- Strengthen strategic litigation as a means of testing the effectiveness of data protection laws and developing African jurisprudence.
- Create structured channels for civil society participation in regulatory investigations, consultations and policy development.
- Expand digital rights and data protection education so that African users understand their privacy rights and available remedies.
- Strengthen the capacity of civil society to monitor regulatory settlements and enforcement outcomes after cases have concluded.
- Build stronger networks connecting African privacy lawyers, civil society organisations, academics and technical experts across jurisdictions.
- The goal should be to move from a model where citizens are merely subjects of data protection to one where they are also participants in enforcing it.

Pillar 6

Recommendations:

STRENGTHEN CORPORATE ACCOUNTABILITY AND PRIVACY BY DESIGN

Big Tech accountability should not begin only after a violation has occurred. Technology companies should be expected to integrate privacy, transparency, accountability and user protection into the design and governance of their products and services. The Summit specifically highlighted privacy by design and the need to elevate data protection to board-level corporate governance.

Strategic Priorities:

- Require major platforms to implement privacy by design and by default throughout the technology lifecycle.
- Require boards and senior management to assume clear responsibility for data protection and privacy governance.
- Require meaningful and demonstrable consent, particularly where platforms seek to link or combine data across different services. The Meta and WhatsApp experience in Uganda demonstrated how regulatory intervention can produce concrete changes in consent practices.
- Strengthen requirements for transparency regarding data collection, processing, sharing and retention.
- Require appropriate privacy and data protection impact assessments for high-risk technologies and large-scale processing.
- Develop stronger standards for algorithmic accountability and auditability, particularly where automated systems affect individuals' rights or access to services.
- Encourage professional associations and privacy practitioners to develop and uphold ethical standards for privacy practice.

Pillar 7

Recommendations:

JUDICIAL CAPACITY AND REMEDIES

African judiciaries should strengthen their capacity to adjudicate privacy and data protection disputes involving powerful data controllers and processors, including Big Tech, while developing jurisprudence that gives practical meaning to data protection rights. The discussions highlighted that judicial competence grows through exposure to cases, continuous capacity building and the willingness of data subjects and practitioners to bring privacy disputes before the courts.

Strategic Priorities:

- Strengthen continuous judicial training on privacy, data protection and emerging technologies, including the business models and data practices of Big Tech platforms.
- Encourage the development of African data protection jurisprudence through cases that clarify the rights of data subjects and the obligations of controllers and processors.
- Strengthen access to judicial and administrative remedies for data subjects, including clear interaction between regulatory complaint mechanisms, judicial review and civil proceedings.
- Encourage courts to interpret data protection legislation alongside sector-specific laws and constitutional privacy protections, allowing courts to address complex data practices through a comprehensive legal framework.
- Promote strategic privacy litigation capable of testing emerging questions involving technology companies, data controllers and processors, thereby creating precedents that strengthen accountability across jurisdictions.
- Increase public and professional awareness of data protection rights so that more data subjects are able to identify violations and pursue appropriate remedies, thereby creating greater opportunities for courts to develop the law.
- Develop stronger judicial dialogue across African jurisdictions, enabling courts to learn from emerging decisions on privacy, personal data and technology-related harms.

Conclusion:

The Seven Pillars emerging from the Summit therefore provide a framework for moving from principle to practice. They point towards a future in which African data protection is not merely about compliance on paper, but about real accountability, meaningful remedies and institutional power capable of holding even the world's most powerful technology companies to account.

The BTA Summit 2026 was therefore not simply a conversation about the challenges Africa faces. It was a call to action for African institutions to build capacity, for regulators to enforce proactively, for courts to develop the law, for professionals and civil society to organise, for technology companies to take responsibility, and for African countries to work collectively to shape the digital environment in which their citizens and economies increasingly operate.

The future of Africa's digital economy must not be defined only by those who build the platforms. It must also be shaped by those whose data, rights, businesses and societies make those platforms possible.

Report Compilation:

This report was compiled by AdLegal International, the convenor of the Africa Big Tech Accountability Summit. As convenors of the Summit, AdLegal compiled this report to preserve the key contributions of participating regulators, practitioners, judges, businesses, civil society and other experts, and to contribute to the continuing development of Africa's data protection and big tech accountability agenda.

Contacts:

Aziz Kitaka
Member, AdLegal
Contact:
ed@adlegalug.com

Luke Kamoga
Member, AdLegal
Contact:
luke@adlegalug.com

Patience Ayesigye
Member, AdLegal
Contact:
patience@adlegalug.com

Nicholas Murere
Member, AdLegal
Contact:
nicholas@adlegalug.com

#AdLegal

www.adlegalug.com

info@adlegalug.com
bta@adlegalug.com

BTA SUMMIT

AFRICA BIG TECH ACCOUNTABILITY SUMMIT 2026
Kampala, Uganda