AFRICAN ACADEMIC NETWORK ON INTERNET POLICY

www.aanoip.org

DATA DATA PRIVACY AND SECURITY IN AFRICA: BUILDING AN EVIDENCE BASE AND A MULTI-STAKEHOLDER ACTION BASE FOR PERSONAL DATA PROTECTION IN NIGERIA

in partnership with

Google, Worldwide Web Foundation, Paradigm Initiative and the Ibadan School of Government and Public Policy

Venue
The International Institute for Tropical Agriculture (IITA), Ibadan, Nigeria

Supported by
Google

Date
04 - 05 Dec 2017

WWW.
AANOIP.
ORG

Hashtags

#AANOIP2017, #DataPrivacy, #Data-

Protection & #DataSecurity

Twitter handle: @AANOIP

.

LIST OF ABBREVIATIONS

AFRINIC	African Network Information Centre
AANOIP	African Academic Network on Internet Policy
ATI	Access to Information
AU	African Union
CLO	Civil Liberty Organization
CPM	Critical Path Method
CSO	Civil Society Organization
DND	Do Not Disturb
ECOSOC	United Nations Economic and Social Council
EU	European Union
EVC	Electronic Verification Code
FoE	Freedom of Expression
FoI	Freedom of Information
GDPR	Global Data Protection Rule
ICT	Information Communication Technology
ICCPR	International Covenant on Civil and Political Rights
IITA	International Institute for Tropical Agriculture
IT	Information Technology
IPv	Internet Protocol Version

LIST OF ABBREVIATIONS

ISPSS	Ibadan School of Government and Public Policy
OECD	Organization for Economic Cooperation and Development
NCC	Nigerian Communications Commission
NGO	Non-Governmental Organizations
NHRIS	National Human Right Institutions
NIRA	Nigeria Internet Registration Association
NITDA	National Information Technology Development Agency
SME	Small and Medium Enterprises
SADC	Southern African Development Community

LIST OF APPENDICES

AFRICAN
ACADEMIC NETWORK
ON INTERNET POLICY

AFRICAN ACADEMIC NETWORK ON INTERNET POLICY

AN OVERVIEW

The Network was established for interdisciplinary scholarly engagement and discussions on the State of the internet, related policies and regulatory regimes in Africa to create a critical mass of Pan-African academic scholars and policy practitioners who would shape the digital economy in Africa.

OBJECTIVES

- Grow African voices to inform digital transformation in the region.
- Provide objective, independent and politically neutral advice to relevant stakeholders on the use of the digital space based on research evidence.
- Pave way for a favourable digital ecosphere for online players.

METHODOLOGY

- Conduct of Seminars and conferences rotated throughout Africa with focus on Nigeria in its first three years of existence
- Provision of Research Leadership through Publications
- Creation of Policy Briefs on topical issues relating to the digital space

CRAFTING THE AGENDA

01 MATTERS ARISING

- Extent of privacy infringement by the government.
- State of cybersecurity infrastructure in Nigeria.
- Availability of frameworks for reaching the Government on the outcomes of the Colloquium in order to have the desired impact.
- Efforts being made to integrate other African scholars and academics in Data protection and security into the network.

05 PANEL RESPONSE

A leading member of the steering committee noted that mechanisms has been put in place for Government engagement through the attendance of government agencies such as NITDA, NIRA, the media and NCC at the Colloquium.

The Ibadan School of Governance and Public Policy (ISGPP) also had a system of continuous interaction with Government. This was complemented by the involvement of other categories of stakeholders such as the legislators, students and communication experts who could drive the advocacy agenda.

It was recommended that Behavioural scientists should also be incorporated into the network because some of the trends in the use of the cyberspace were not strictly matters of legislation.

WELCOME ADDRESS BY DR. TUNJI OLAOPA, EXECUTIVE VICE-CHAIRMAN, ISGPP

Due recognition to the key partners namely: Google represented by Titi Akinsanmi, The Web Foundation represented by Nnenna Wakama, Paradigm Initiative represented by Tope Ogundipe and the keynote speaker in the person of Dr. Ololade Shyllon from the Centre for Human Rights, Faculty of Law, University of Pretoria, members of the Board of ISGPP especially Mrs. Ify Chukwuma and some other strong partners of the ISGPP, namely Professor Ayo Olukotun and Professor Umaru Dambatta as well as representatives of the EVC and NCC. He further acknowledged their individual and collective roles in the evolution of the African Academic Network into its current shape and expressed his optimism for the massive possibilities of the imminent collaborations that would shape the future of the Digital Economy in Africa through the activities of the organization.

The Ibadan School of Government and Public Policy is a growing independent think-tank and had been highly instrumental to the evolvement of the African Academic Network in Internet Policy through its multidisciplinary Public Policy Group which comprises over 150 leading expert-members in critical policy research domains and activities such as Policy Dialogues, Book reading events, graduate programmes, Executive Education and Seminar series on topical issues.

The Roundtable discussion held in May, 2017, was to highlight ways of addressing the challenge of strengthening Internet Policy through Theoretically Grounded research. The current meeting, which addresses Data Privacy and Security: Building the Evidence Base and a Multi-Stakeholder Action base for Personal Data Protection as one of the thematic areas of the Network, is the first attempt to pick up the pieces of the big gaps that had been identified at the earlier meeting. This meeting is designed to a focus on Data Privacy and Security and the ultimate aim of getting research based and practice oriented content across to the right stakeholders.

The emerging African Academic Network on Internet Policy is a Pan-African academic network on Internet and Digital Policy which leverages the rigour of localized researches and their application to drive the growth of the African Digital Economy within the following thematic areas: State and the Individual: Privacy and Cyber Security, Copyright: Fair use and IP protection, Data Driven Innovation in a Developing Economy, the Politics of governing the Internet / political dynamics in Internet governance, Internet Policy and its development impact as well as the Role of Institutions in the governance of the Internet, among others.

It is our strong desire that some of the outcomes of the Colloquium would be a template for a more systematic and synergistic engagement by the African Academic Network and a solution framework for further research and policy conversations that stakeholders would readily take advantage of to drive the consolidation of the digital economy in Africa.

2.0

THE LEGAL FRAMEWORK FOR THE PROTECTION OF THE RIGHT TO PRIVACY AND DATA PROTECTION IN AFRICA: CHALLENGES AND PROSPECTS

By Dr. Ololade Shyllon on 4th December, 2017

Major Information-related rights

- Freedom of Expression;
- Access to information;
- Privacy / Protection of Personal Information.

Rights Appertaining to Data Subjects

- Right to information;
- Right to access;
- Right to object;
- Right of rectification or erasures of misleading information

The basic principles governing data processing are as follows:

- **Consistency and legitimacy**
- **Lawfulness and fairness**
- **Purpose, relevance and storage**
- **Accuracy**
- **Transparency**
- **Confidentiality and security**

Human rights are "rights we have by virtue of being human" and having the major characteristics of being universal, indivisible, interdependent and inter-related.

The State has the primary responsibilities of respecting, protecting and fulfilling the commitments of ensuring that the citizenry do not have their rights violated.

Challenges with existing regional and national data protection frameworks in existence

01

There is a worrisome trend created by Exceptions in the AU Convention, Supplementary Act and the SADC Model Law.

02

Conceptualization of protection of personal information strictly as an ICT issue

03

Exemption of important categories of personal information

04

Reliance on dated data protection standards from other regions

05

Lack of Regional Mechanism to Monitor Implementation

MEASURES TO ENHANCE STRONGER DATA PROTECTION

RECOMMENDATION

Adoption of a data protection law that:

borrows from the most recent legal frameworks on data protection such as the EU Guidelines 2016 and revised OECD standards 2013.

takes into account Nigeria's international obligations on privacy and other human rights, especially under ICCPR

takes into account domestic laws, Constitution, the FOI Act and other relevant laws

takes into account international best practice on privacy e.g. consider combining implementation of FoI

2.1

PERSONAL DATA PROTECTION IN NIGERIA

Barrister Chukwuyere Ebere Izuogu On 5th December, 2017

OBJECTIVE:

To identify the main data protection risks in Nigeria and recommend policy options for reforming the data protection ecosystem.

Although, Nigeria does not have a (personal) data protection law of general application, it was embedded in Section 37 of her Constitution that "The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected"

Personal data is defined as any information relating to an identified or identifiable natural person and examples of such include: Personal name, Facial photograph, Biometric information, IP address, GPS position, Sexual orientation, Religious beliefs and Bank account statement, among others. (European Union Data Protection Law)

INTERACTIONS WITHIN THE PERSONAL DATA PROTECTION

The Data Subject

Provides their personal data for processing

The Data Controllers

Determines the purpose and means of processing the personal data

The Data Processors

Processes personal data on behalf of the data controller

Third Parties

Receives personal data from a data controller of data processor

DATA PROTECTION REGULATORY FRAMEWORK

Organisation for Economic Co-operation and Development (OECD) Guidelines Governing the Protection of Privacy and Trans Border Flows of Personal Data 2013 (International)

African Union Convention on Cyber Security and Personal Data Protection 2014 (International)

The Economic Community of West African States Data Protection Act 2010 (International)

Protection of Personal Information Act 2013 (South Africa)

Data Protection Act 2012 (Ghana)

The General Data Protection Regulations (European Union wide)

MAIN ELEMENTS OF A DATA PROTECTION REGULATORY FRAMEWORK:

·Fair and lawful processing.
·Purpose specification
·Relevant (or data minimization)
·Accuracy
·Non-Retention beyond need for use
·Data subject rights (including the right to be forgotten/erasure),
·Data security and accountability

DATA PROTECTION RELATED INITIATIVES IN NIGERIA

SECTION 37 OF THE CONSTITUTION OF THE FEDERAL REPUBLIC OF NIGERIA:

"The privacy of citizens, their homes, correspondence, telephone conversation and telegraphic communications is hereby guaranteed and protected"

SECTION 5 OF THE CREDIT REPORTING ACT 2017:

"A Credit Bureau shall maintain credit information for not less than 6 years from the date on which such credit information was provided to it, or if later, on the date on which it last provided such information to a credit information user"

SECTION 38 (4) OF THE CYBERCRIME ACT 2015:

"Any data retained, processed or retrieved by the service provider at the request of any law enforcement agency under this Act shall not be utilized except for legitimate purposes as may be provided for under this Act, any other legislation, regulation or by an order of a court of competent jurisdiction".

REGULATION 9 (4) OF THE NIGERIAN COMMUNICATIONS COMMISSION REGISTRATION OF TELEPHONE SUBSCRIBERS REGULATIONS 2011:

"Licensees, Independent Registration Agents, Subscriber Registration Solution Providers and the Commission shall each take all reasonable precautions in accordance with international practises to preserve the integrity and prevent any corruption, loss or unauthorised disclosure of subscriber information obtained pursuant to these Regulations and shall take steps to restrict unauthorized use of the Subscriber Information by their employees who may be involved in the capturing or processing of such subscriber information

MEASURES BY WHICH THE PROCESSES OF DATA COLLECTION AND USAGE IN NIGERIAN CAN BE CORRECTLY POSITIONED

Legislative measure – Data Protection and Child Online Privacy Protection Acts should be enacted while the National Identity Management Commission (NIMC) Act should be amended to incorporate robust data protection principles and expand the powers of the NIMC to function as a data protection authority.

Non-legislative (soft law) measures to enable the NIMC undertake administrative rule-making should be put in place

Judicial measures including encouraging superior courts of records in Nigeria to engage in judicial activism should be explored

SUMMARY OF DATA PROTECTION RELATED ISSUES

	Offline	Online
TYPE OF DATA COLLECTED	Name, Fingerprints, Facial photographs, Residential address, Telephone number, and Health information	Name, Email address, Internet Protocol (IP) address, Click stream data, Telephone number, Location information and Sexual preferences
EXAMPLES OF ORGANIZATIONS THAT COLLECT EACH DATA CATEGORY	National Identity Management Commission (NIMC), Independence National Electoral Commission, (INEC), National Immigration Service (NIS), Vehicle Inspection Office (VIO), Banks and financial institutions, Hospitals/ Health Management Officers (HMOs)	Google, Youtube, Facebook, Twitter, Whatsapp, Xvideos, Truecaller, ISPs
DATA PROTECTION RISKS	Incompatibility of purpose, Data subjects have no rights in relation to their personal data	Lack of adequate consent-Consent must be informed, freely given and specific, Lack of transparency in the processing of personal data- The data subject is in a fog of data ignorance, Lack of security and risk of a personal data breach, Incompatibility of purpose, Children are overly exposed to privacy risks online

Enforcement measures- The National Human Rights Commission should be engaged to enforce data protection cases while the Consumer Protection Council, NIMC and other regulators should be mandated to address the unscrupulous exploitation of consumers and uphold the highest ideals of data management

Executive measures to harmonize institutional efforts and remits should be put in place by the Federal Government

Social measures to include participation of Civil Society Organizations and the general public in raising awareness on data privacy and security from a human rights' perspective should be widely embraced.

3.0

PRESENTATION OF THE PERSONAL DATA PROTECTION REPORT IN NIGERIA

Nnenna Nwakanma (Rep, The Web Foundation)

OBJECTIVE:

One of the main challenges of using the web is digital trauma arising from digital insecurity.

Against this backdrop, the web foundation was created. The Web Foundation's interest in Nigeria is borne out of the fact that Africa is one of the world's emerging markets and Nigeria as the most populous nation in Africa is key in the use of the internet and in building a framework for data privacy and security in Africa. The Webfoundation recently undertook a study on Personal Data Protection in Nigeria which had Barrister Chukwuyere Izuogu has the Principal Investigator and from which the second Keynote presentation for the Colloquium was drawn.

THE POLICY RECOMMENDATIONS WHICH EMERGED FROM THE STUDY ARE:

Use of personal data must be in accordance with the purpose for which it was collected (purpose specification)

Consent of the individual must be obtained prior to collecting his or her personal data

Rights of the individual to seek legal redress for misuse and / or unauthorized access to his / her personal data must be guaranteed.

The recommendations could be addressed through legislative (National Assembly intervention), non-legislative (soft law), judicial, enforcement, executive and social measures.

Key Findings of the Report

There is limited-to-no transparency around the processing of personal data and there is limited information available around how this personal data is used and stored, leading to greater risk of a personal data breach

The use of personal data may be incompatible with the purpose for which it was collected;

Individuals have no rights in relation to the collection, use and storage of their personal information;

Nigerians are not offered adequate opportunities to consent or opt out of data collection;

Children are exposed to privacy risks online and often lack the legal capacity to give valid consent. They may also unknowingly disclose personal information to online platforms due to the appealing nature of their visual content.

4.0 WHY DATA PROTECTION?

Plenary Session One

Google Policy Group Lead.	IP Engineer, CEO of General Data Engineering Services, Chair of Board of AFRINIC and NIRA	Solicitor, Africa and Vice-Curator with World Economic Forum	Attorney with Webber Wental in Johannesburg; specializes in Campus data Privacy issues	Immediate Past Executive Director, Data Protection Commission, Ghana, Senior Partner
Mrs. Titi Akinsanmi	Rev. Sunday Folayan	Barr. Chuka Ajuluchukwu	Ms. Okyereba Ampofo	Mrs. Teki Akuetteh Falconer

Institution
Names of Panelists

Aims & Objectives of the Session

- To highlight the importance of Data Protection by cyber space users in Africa
- To identify Data protection related initiatives including existing and proposed laws and regulatory frameworks in Africa
- To evolve strategies for better compliance with Data Protection Regulations in Africa

Key Points from Presentations

- Trends drive policy on data protection
- Practical solutions have to emerge from the Colloquium without compromising academic content
- Conflict of interest at personal vs. professional and national vs. international levels could interfere with enforcement of regulations
- Trust-building with stakeholders is key to the successful collection and release of Data by their end-users
- African businesses dealing with European partners need to be correctly positioned to remain in business post implementation of the European Global Data Protection Rule (GDPR) in 2018 especially in view of the heavy fines associated with violation of Data Protection rules
- Privacy is a non-negotiable human right

Challenges Identified

- Weak enforcement and operationalization of the by-laws and regulations such as the NCC consumer code of practice
- Lack of proper understanding of the Data Privacy Landscape in Nigeria as evidenced by posting of personal information in places of interest to predators by people in need of protection
- Unclear methodologies for balancing in practice the compliance requirements of data protection
- Businesses with IPv addresses traceable to Nigeria are frequently blocked from the international e-commerce sites

Recommendations

- Regular training and capacity building for all stakeholders involved in data protection at all levels
- Knowledge and awareness has to be created on the importance of data privacy
- Efforts must be improved on clarity of methodologies on the adoption of Data Protection regulations to ensure compliance.
- Assistance should be provided to small and medium enterprises (SMEs) to learn how to mitigate risks associated with compliance with data protection rules

4.0
DISCUSSION ON KEYNOTE PRESENTATION I

Plenary Session Two

Session Facilitator:
Tope Ogundipe (Paradigm Initiative)

Manager, Legal Services, National Information Technology Authority, Uganda	Research Manager, Research ICT Africa	Deputy Head, Cyber Security/ Cyberware Intelligence and Operations; and the Professor of Cyberwarfare, National Defense University	Head, Cybersecurity Unit, NCC	Senior Associate, Streamsowers and Kohn
Barbarah Imaryo	Enrico Calandro	Prof. Kris Seeburns	Engr. Abubakar Meina	Barr. Chukuwyere Izuogu

Institution
Names of Panelists

Goal of the session

- to brainstorm on the way forward in ensuring maximum data protection for African citizens from a human rights perspective

Key Points from Presentations

- Sections 34, 8 (of the Child Act) and 14 of the Constitution of Nigeria contain information on how the rights of citizens with respect to their personal data are protected
- Citizens have a right to know details of the kinds of data the State / Government is seeking to access about them and obtain legal redress where necessary
- A multi-stakeholder approach is required to ensure that the rights of citizens for data protection are respected and upheld
- Gender issues should be mainstreamed into the enforcement of data protection rights early.

Challenges Identified

- Nigeria does not have any Data Protection Act presently
- There is inadequate cooperation with the FoI Act
- Frameworks for accountability and compliance do not really exist for rights to privacy
- Access to information and privacy are not yet seen as human rights issues in most African countries
- The legal frameworks for safe trans-border flow of data and information are inadequate
- The ratification of the AU convention is appallingly low

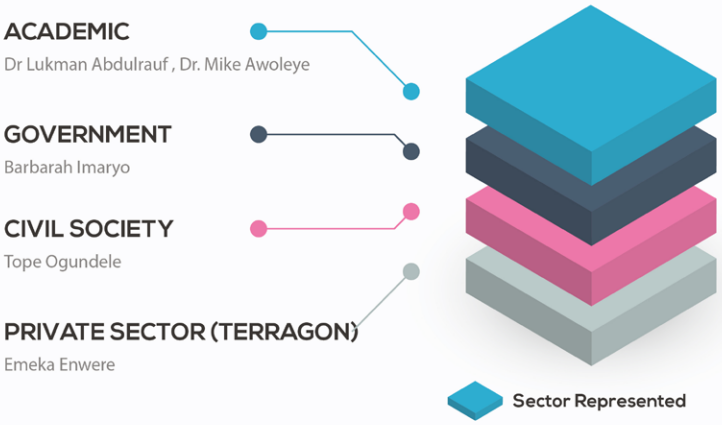
Recommendations

- There should be proper oversight on activities of Government seeking to access data of private citizens for law enforcement purposes to prevent abuse
- Boundaries of jurisprudence need to be pushed for data protection when there is a basis for doing so
- Nigerians need to be familiar with the constitutional provisions for the protection of their data and maximize same
- A multi-stakeholder approach is necessary to enforce compliance with data protection regulations
- They Cybercrime Act, though presently inadequate, needs to be put into practice so that areas of insufficiency can be identified and addressed early
- Awareness, advocacy and technical support should be raised about the data protection human rights issues around the AU convention

4.1 WHY DATA PROTECTION?

Panel Session / Discussions on Keynote Presentation II

Moderator: Nnenna Nwakanma



Goal

- To discuss the outcomes of the Personal Data Protection in Nigeria Report with a view to advancing a strategy for progressive action

Key Points from Presentations

- Although there is no general data protection law in Nigeria, the sectoral laws are equally important.
- It is pertinent for Nigeria to commence setting up mechanisms that will harmonize and synchronize the data of its citizenry using the appropriate technologies
- Data protection as a human rights issues transcends its economic and political considerations.
- Data peddlers are on the rise in Nigeria and this is a major impetus for increasing awareness of data protection and privacy issues among relevant stakeholders
- Legislative, Non-legislative, Executive, Judicial and Social measures all need to come on board to ensure adequate data protection in Nigeria
- The NCC is making giant strides in the direction of data protection by creating a DND application and launching a platform for addressing complaints on unlawful interception of data

Challenges Identified

- The bureaucracy involved in rectifying errors on personal data collected by government agencies is alarming (e.g. correction of Bank Verification Number (BVN) details)
- Sometimes, important data such as Driving License application information can actually be lost and it may be difficult to hold a particular person or agency responsible

Recommendations

- Data protection laws must be more objective than subjective.
- Data collectors must be checked from absolving themselves of all responsibility on the data in their possession.
- Measures should be put in place to enforce compliance with existing Data protection laws rather than hurrying to enact new law.
- There should be accelerated efforts in respect of building infrastructure for hosting data for Nigeria and Nigerians in Nigeria.

STRENGTHENING KNOWLEDGE BASE/CAPACITY ON DATA PRIVACY AND SECURITY

Lead: AKUETTEH Teki

Goal: Developing an Afro-Centric Capacity Building Program/Curriculum on Data Privacy and Security.

Challenges Identified:

1. Developing an Afro-Centric program for capacity building in data protection and privacy.

2. Gaining traction or credibility for an African Certification especially in the context of international standards.

3. Engaging universities across Africa to build data protection programs.

4. Crafting the right strategy in approaching data protection and privacy issues in Africa.

Action Point

Capacity building in data protection and privacy should be approached in two ways: Formal and Informal

The Formal Side:

1. Certification programs must be country-specific i.e. that should apply to each of the countries.

2. Association of African Universities to engage in the certification process and to reach out to universities in Africa.

3. The data protection advocacy process involves sensitizing the key players and generating an output from this process. This medium involves

a. A knowledge park: content that addresses the different layers from researchers to core policy player

b. A communication Strategy – how to get people to buy into it

c. A collaborative driven strategy

4. Incorporating data protection and privacy contents in the curriculum of other courses being taught in the universities.

5. The NCC Model could be adopted by bringing leading practitioners to develop and facilitate content and training systems to create an inclusive based approach.

The Informal Side:

1. To involve the media because the media set the agenda and shape the opinion.

2. Grassroots advocacy i.e. training the critical mass through radio programmes, television shows, social media and other local means to champion the campaign around data protection and privacy awareness.

3. Advocacy groups on campus like clubs driving the buzz around data protection

Data privacy and protection regulation enabling innovation (Focus on Nigeria) on 5th December, 2017

Leads: Nnenna Nwakanma, Chukwuyere Izougu, Emeka Enwere, Dr Temitope Aladesanmi

Goal: Addressing gaps in Law through advocacy

Key Points from Presentations:

1. The goal of data protection is not restricting the use of data rather it is aligning the interests of organizations with interests of data subject

2. The reality of the new information driven world is the penetration of our privacy, the task at hand is defining the extent to which privacy intrusion is allowed.

3. In the long run what is realistic is informed consent on data use rather than absolute privacy.

4. Data protection is a human right interest issue, and it concerns all everyone.

Challenges Identified:

1. How to strike a balance between respect of human rights and innovation in the business space.
2. How to drive social measures that will birth a robust digital policy guideline while simultaneously enabling innovation at the same time.
3. How to define Internet perspective in an African perspective.
4. How to identify and address gaps in law through advocacy.

Action Point

1. Aggressive user education on End- User License Agreements. (EULAs) – CSOs & MDAs
2. Engage the power of infographics in data privacy and security awareness. (Budgit Nigeria)
3. Creation of locally accessible and understandable end-user agreement (MNOs and Telcomms)
4. Engaging the mainstream media is the most potent form of awareness and sensitization. (CSOs)
5. The awareness of data privacy and security must be built into the heart of educational curriculum and content. (Government Agencies)
6. Champion the awareness of data privacy by setting up data privacy and protection ambassadors in tertiary institutions in Nigeria. (CSOs to be led by Mr Emeka Ossai)
7. Policy makers should make building capacity in Science and Technology development a priority. (Government Agencies & MDAs)
8. Aggressive social awareness needs tobeputinplaceintheformofa suitable hashtag campaign in the coming weeks (AANIOP, The web foundation)
9. 1. Civil Society Organizations (CSOs) should commission further reports in data privacy and security issues thereby leading advocacy on the subjects.

Mainstreaming and Driving thought leadership on Data Privacy and Security.

Leads: Professor Muta Tiamiyu, Tope Ogundipe

Goal / Objective: Advocacy Strategy for sustained engagement with Public and Government through Media

Action Points

1. awareness of citizens around privacy rights through social networking sites, Radio/TV communication, town hall meetings, FGD/workshops with opinion leaders.
2. There is the need for government to legislate, enforce
3. and implement data privacy/protection laws.
4. There is the need for government to create awareness and provide resources for implementation of data privacy/protection laws through social media and policy briefing.
5. There is the need for private organizations to create awareness and ensure compliance through annual reporting, stakeholders' meetings, workshops, seminars, conferences and social media hash tags.
6. There is the need for relevant international and regional bodies to harmonize data protection
7. laws through lobbying, stakeholders' meetings, social media and reporting.
8. There is the need for relevant international and regional bodies to create a framework for data protection through stakeholders' meetings.
9. There is the need for relevant international and regional bodies
10. to update and review data protection laws and encourage state members to ratify sub- regional instruments.

SUMMIT SUMMARY

African Academic Network on Internet Policy in Partnership with Google and World Wide Web Foundation 2 Days' Colloquium/Seminar held at the International Institute for Tropical Agriculture (IITA), Ibadan, Nigeria from December 4-5, 2017.

Background Information

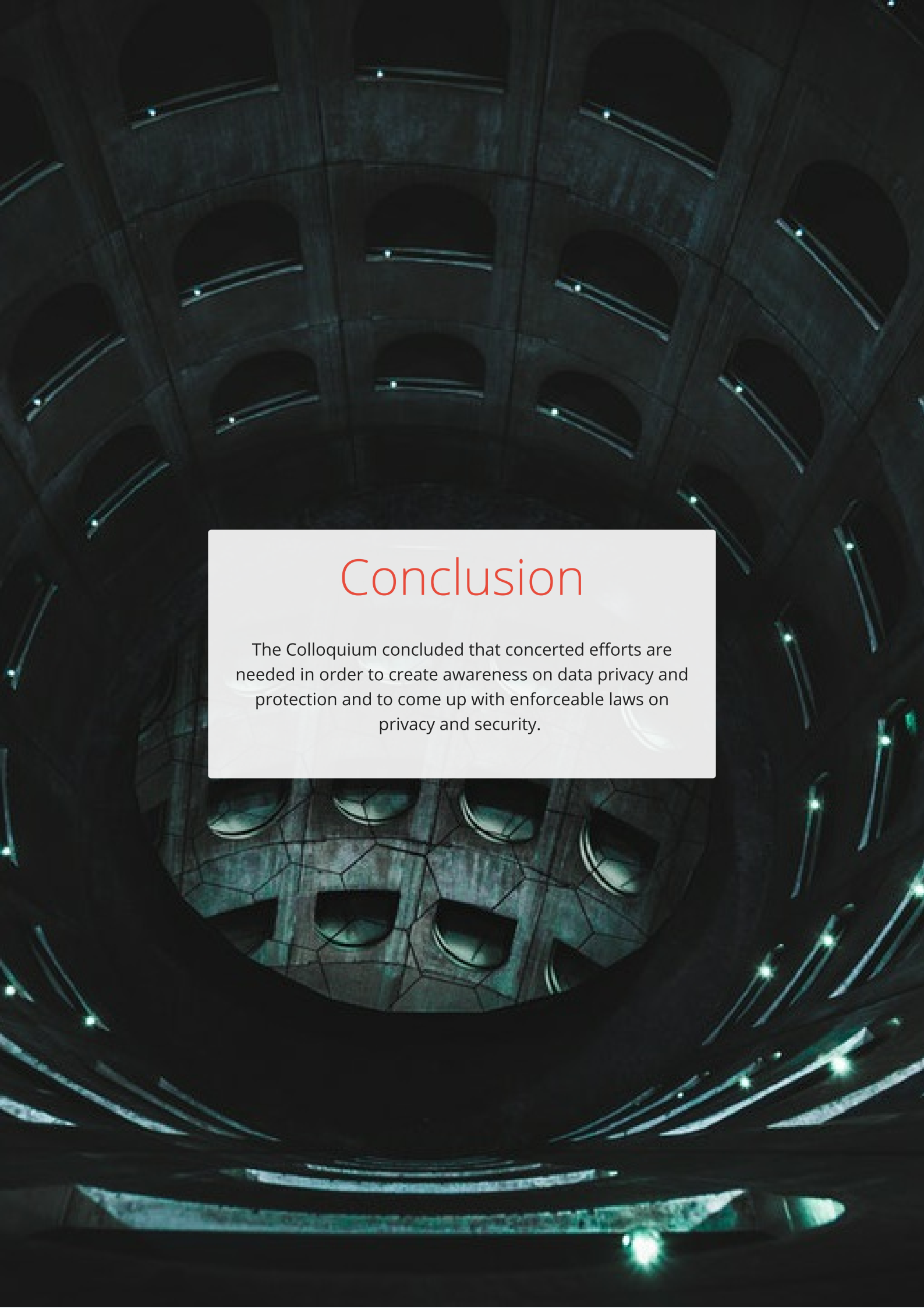
Seventy seven (77) Delegates comprising leading ICT professionals, Legal experts, Policy practitioners, Academics, Representatives from Civil Society, Students and other key stakeholders on issues of Data Privacy and Security from Kenya, Uganda, Mauritius, South Africa, Ghana, Nigeria, Cote d' Voire, and the United States of America gathered at the International Institute for Tropical Agriculture in Ibadan, Nigeria, to stimulate discussions on the state of Data Privacy and Security from a Human Rights perspective with a view to building the evidence base and multi-stakeholder framework for data protection over a 2-day period.

Aims/Objectives of the Colloquium

- To consolidate the emerging African Academic Network on Internet Policy
- To brainstorm on pertinent issues relating to data privacy and security in Africa.
- To bring into focus crucial dialogues, discussions, presentations, debates and resolutions on some of the important challenges of data privacy and security in Africa.
- To facilitate the collaborative development of actionable next steps on the basis of identified gaps and best practices within the context of the local environment

Outcomes of the Colloquium

- Generation of thought leadership on increasing awareness of data privacy and security issues through a combination of academic and advocacy engagement.
- Increased understanding of data privacy and security issues from a human rights perspective
- Assessment of the adequacy of protection under the existing data protection framework in Nigeria vis- a-vis other African countries
- Proposition of an impactful and measurable strategy for the development, review or adoption and effective enforcement of relevant laws and regulations
- Advocacy for a capacity building strategy to grow the knowledge base of key sectors and stakeholders in Africa's digital economy



Conclusion

The Colloquium concluded that concerted efforts are needed in order to create awareness on data privacy and protection and to come up with enforceable laws on privacy and security.