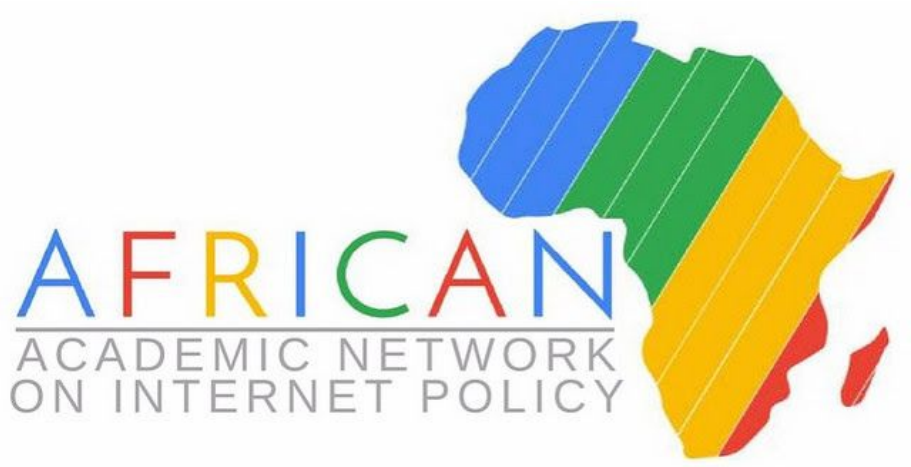

SEMINAR SERIES BRIEF

Theme: ***Data Privacy and Security: Building the Evidence Base and a multi-stakeholder action base for Personal Data Protection***

Date: December 4 - 5 2017

'The world's most valuable resource is no longer oil, but data'
Forbes News

'Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety.'
Benjamin Franklin

'You have to fight for your privacy or you will lose it.'
Eric Schmidt

THE AFRICAN ACADEMIC NETWORK ON INTERNET POLICY

The African Academic Network on Internet Policy, hosted by the Ibadan School of Government and Public Policy (ISGPP), Nigeria is a network for interdisciplinary scholarly engagement and discussion on the State of the Internet, related policies and regulatory regime in Africa. As part of its mandate, the AANIP hosts seminar series / colloquiums to bring into focus and to foster discourse on crucial issues as it connects ot the digital economy - driven by the Internet.

The Colloquium convenes African stakeholders drawn from Academia, Government and the private sector. Over the course of two days, there will be presentation of papers based on research carried out by academics. This would be followed by panel discussions reviewing the issues identified in the report - which then inform breakout sessions tasked with the goal of identifying and presenting related next steps and action plans for the network and attending stakeholders.

The first of these Seminar Series is focussed on ***Data Privacy & Security*** and themed ***'Building the Evidence Base and a multi-stakeholder action base for Personal Data Protection'.***

WHY DATA PROTECTION, PRIVACY AND SECURITY?

In the global information economy, personal data is the 'fuel' powering online activity and growth offering 'A Trillion Dollar Opportunity' for individuals, corporations and sovereign states[1]. Each day, a vast amount of information is transmitted, stored and collected across the globe, enabling innovations in computing, applications development and user focussed deployment. The latter is primarily driven by the exponential adoption and use of mobile technologies, increasing access to the Internet and an appetite for knowledge related to social, economic and financial activities - moreso on the African continent, with AU Agenda 2063 recognising the Digital opportunity.

As more and more economic and social activities move online, the importance of data protection and privacy; its ethical use and protection is at the forefront of the agenda of many countries, not least in the context of international trade[2] [3]. At the same time, the current system for data protection is highly fragmented, with diverging global, regional and national regulatory approaches. Internationally compatible data protection regimes are desirable as a way to create a collaborative and innovative environment and to enhance cooperation and trust online and across borders.

New technological developments are adding urgency to this need. Cloud computing is rising in prominence as defacto option to efficient and effective data storage, disrupting traditional

[1] **Franklin F Akinsuyi,** (April 15, 2015)"Data Protection & Privacy Laws Nigeria, A Trillion Dollar Opportunity" available at: https://www.linkedin.com/pulse/data-protection-privacy-laws-nigeria-trillion-dollar-f-franklin

[2] **UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT Report** on Data protection regulations and international data flows: Implications for trade and development available at: http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_summary_en.pdf

[3] **The European Union General Data Protection Regulation** available at: https://www.eugdpr.org

models in various areas of law, business and society. Projections estimate that the cloud computing industry will have a projected global market worth of $107 to $127 billion by 2017[4].

The Internet of Things is also rapidly developing, and has a direct nexus to management of data. While forecast reports vary greatly, one report estimates that value-added services related to the Internet of Things will grow from around $50 billion in 2012 to approximately $120 billion in 2018, and that there will be between 20-50 billion connected devices by 2020. Another report forecasts a potential economic impact of between $3.9 and $11.1 trillion per year in 2025[5].

The processing of personal information is a basic building block for the 21st Century and new applications of data analytics show its tremendous potential value for informing and accelerating sustainable development - ranging from economic well being, education, public health, migration to climate change. Transborder data flows have reinforced the need for countries to build the infrastructure to be part of a global information ecosystem. Thus, a necessary 'infrastructure' is reviewing and where needed shaping a regulatory and policy system, which adequately addresses new data uses across economic sectors.

Although there is significant divergence in the detailed data protection laws of the world, there is greater consensus around the core set of data protection principles at the heart of most national laws and international regimes. These include the principle of openness, collection limitation, adequate purpose specification, use limitation, security, data quality, access and correction and accountability.[6]Some data protection regimes apply equally to all those processing personal data while others apply different rules to specific sectors (e.g. health industry), types of processing entity (e.g. public authorities) or categories of data (e.g. data about children).

BACKGROUND PAPERS FOR DISCUSSION

This section is a summary of the two independently commissioned research papers. Each paper gives an overview of existing laws[7], policies and related legal agreements that speak to Data Privacy and Security at the continental level with a day of discussion dedicated to the Nigerian case study. Over

Paper 1: Data Privacy and Security in Africa

The digital age has brought to the fore the impact of information and communication technologies (ICTs) on the promotion and protection of human rights, especially the three information related rights of freedom of expression, access to information and privacy. While the

[4] **2016 Top Markets Report Cloud Computing** by International Trade Administration available at: https://www.trade.gov/topmarkets/pdf/Cloud_Computing_Top_Markets_Report.pdf

[5] **UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT Report** on Data protection regulations and international data flows: Implications for trade and development available at: http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_summary_en.pdf

[6] T**he OECD Data Protection Guidelines** available at: http://oecdprivacy.org

[7] Data protection and privacy laws have been enacted in over 109 countries as at January 2015. In 2014, the African Union at its 23rd session adopted the Convention on Cyber Security and Data Protection.

realisation of the right to freedom of expression and access to information is significantly aided by the internet and other ICT platforms, these mediums also pose a risk to privacy.

International and regional legal frameworks on the right of access to information recognise that data protection, though most commonly framed as the right to privacy, is a legitimate limitation to the right of access to information. At the same time, there is also international and regional recognition that the exercise of the right to privacy in the context of data protection, requires access to personal information held by public and private institutions.

On the other hand, although the development of data protection standards began initially as a reaction to perceived threats to personal information posed by the activities of the ICT sector, today, these standards have been further expounded and are implemented within the framework of international human rights norms. In Africa however, the development of normative standards on privacy continues to take place within the (ICT) sphere, without due regard to human rights. This approach is further exacerbated by the absence of the right to privacy in the regional human rights treaty, the African Charter on Human and Peoples' Rights. Beyond this, several normative gaps have been found within existing data protection laws at the regional and domestic level in Africa.

To address this, various recommendations at the international, regional and domestic level are made. These include engagement with international processes and mechanisms such as: the State reporting processes of the Human Rights Committee, the Universal Periodic Review Process and with the Special Rapporteur on the Right to Privacy. At the regional level, recommendations are strategically focused on mainstreaming data protection into the work of the African Commission on Human and Peoples' Rights and other human rights mechanisms. Recommendations are also made to private actors operating to develop and strengthen internal policies and processes in a manner that entrenches a human rights based approach to data protection in their activities[8].

Paper 2: Personal Data protection in Nigeria

In Nigeria, privacy is a fundamental human right guaranteed by the Constitution of the Federal Republic of Nigeria (the Constitution), unfortunately, there is yet to be enacted a comprehensive data protection legislation, even though several government and private organizations routinely collect and process personal data. Instead, the existing regulatory frameworks that will arguably apply to the protection of personal data are the broadly phrased Section 37 of the Constitution which provides that: "*The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected*", and a hodgepodge of other industry (or situational specific) frameworks such as the National Health Act applicable to health records, the Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations applicable to the communications sector and the Bank Verification Number (BVN) policy applicable within the financial services sector.
Although these regulatory frameworks are consistent with the data protection principle of lawful processing of personal data and in at least one case, expressly sets the limit on how personal

[8] **Dr. Lola Shyllon** (2017) Executive Summary Commissioned Research on The Data Privacy and Security Landscape in Africa

data collected in this Study, “personal data”, “personal information” and “personally identifiable information” are used interchangeably)may be used (purpose specification). However, most of these frameworks do not clearly define the level of protection afforded to the personal data collected, state the data controller’s accountability obligation(s) or contain any other data protection principle as is the norm in the data protection legislation of other countries.

The Study is a comprehensive review and analysis of the existing and proposed regulatory frameworks that applies to the collection and/or protection of personal data in Nigeria, with recommended policy options for reforming the data protection ecosystem. As stated in the terms of reference and methodology (work plan), the Study has the following objectives;

I. Identification of data protection related initiatives including existing and proposed laws and regulatory frameworks in Nigeria;
II. Identification of the type of personal data collected by organizations both offline and online in Nigeria, and the purpose for which the personal data is collected;
III. Analysis of individuals’ (data subjects) perception of personal data protection through the conduct of a survey
IV. Assessing the adequacy of protection under the existing and proposed data protection framework in Nigeria against a (risk based) model framework for data protection
V. An overall assessment of the national data protection ecosystem in Nigeria, including the deficiencies of the existing personal data protection regulatory frameworks, and detailed identification of the main data protection risks or concerns; and
VI. Recommended policy options for reforming the data protection ecosystem in Nigeria.[9]

Governments specifically in developing countries attempting to adopt data protection legislation are faced with challenges on modeling their data protection regimes.[10] Though most opt for an approach consistent with the EU Directive. Common challenges include:

- the length of time it takes to pass legislation
- financial costs associated with implementing and enforcing a data protection regime
- and a lack of public and private sector knowledge and cooperation among governmental entities regulating in parallel.
- In some countries, a lack of understanding and fear within society can also exacerbate one or more of the aforementioned difficulties.

The Private sector which is primarily at the forefront of the innovative use of data are concerned with the following:

- stringent protection regimes unduly restricting internet economic activities, increasing administrative burdens and stifling innovation;

[9] **Chukwuyere Ebere Izuogu** (2017) Executive Summary Commissioned Research on Personal Data Protection In Nigeria. A Study prepared for the World Wide Web Foundation (Web Foundation).
[10] **Christophe Fichet,** 19 May 2015, A report on Emerging Data Protection regulations in Africa Commissioned by Simmons & Simmons. Available at: http://www.elexica.com

- a lack of clarity and compatibility between regimes add uncertainty, with negative effects on investments; and
- given the nexus between cross-border-commerce and data protection, divergent regimes will inhibit the adoption and proliferation of emerging technological developments, reducing potential accompanying societal benefits.

Numerous challenges in the development and implementation of data protection laws exist. There is a need to concentrate and discuss on the seven key areas where action is particularly needed. These include addressing gaps in coverage and new technologies, managing cross-border data transfers, balancing surveillance and data protection, strengthening enforcement, determining jurisdiction and managing the compliance burden

PANEL DESCRIPTION / METHODOLOGY

Post presentation of each paper, a moderated panel of 3 - 4 will experts will engage with the findings of the paper presenters. The focus of each panel will be contextualized for both Africa and Nigeria on issues related to:

1. Addressing gaps in coverage
2. Addressing new technologies
3. Managing cross-border data transfers and how it affects the Internet's Digital Economy
4. Balancing surveillance and data protection
5. Strengthening enforcement
6. Determining jurisdiction
7. Managing the compliance burden

EXPECTED OUTCOME

The Seminar's overarching goal is to facilitate the collaborative development of actionable next steps. Having identified gaps and best practices (as adaptable and relevant to the local context), four 'action groups' are to be tasked with:

- driving thought leadership through a sustained academic engagement + advocacy programme using media
- developing an impactful and measurable strategy for the development, review or adoption and effective enforcement of law and regulations;
- addressing the disconnect/separation of Data Privacy and Human Rights
- shaping a capacity building strategy to grow knowledge base of key sectors and players.

BREAKOUT SESSIONS

Each Working Group will have about 3-5 experts engaging in open and candid talks on the respective expert area, with a mix of Government representatives, Private Sector Leaders, Civil Society, students and researchers serving as group members and enriching the roundtables with questions and answers. Experts will support their

positions with written papers and presentation from the presenters. There will be a facilitator within each Working Group to ensure the smooth transition through the different formats, harmonise findings and ensure that the intellectual content of the working groups fully captured and articulated.

- Day 1 WG 1: Data Protection & Security - addressing the Gaps in the Narrative (focus on Human Rights (FoE and FoI)
    - Goal:
    - WG Lead: Dr. Lola Shyllon [+ PIN + Okyrebea (?)]
    - Rapporteur:
- Day 1 WG 2: Strengthening Knowledge Base/Capacity on Data Privacy and Security
    - Goal: Developing a Afro-Centric Capacity Building program/curriculum on Data Privacy and Security
    - WG Lead: Teki Akuetteh [+ WWW + PIN + Dr. Walubengo]
    - Rapporteur:
- Day 2 WG 3: Data privacy and Protection regulation enabling innovation (NG Focus)
    - Goal: Addressing gaps in Law through advocacy
    - WG Lead Team: Nnenna Nwakanma + Chukwuyere Izuogu + Terragon + Dr. Aladesanmi
    - Rapporteur:
- Day 2 WG 4: Mainstreaming and driving thought leadership on Data Privacy & Security
    - Goal: Advocacy Strategy for sustained engagement with Public and Government through Media
    - WG Lead: PIN + WWW + Dr. Frempong
    - Rapporteur: