REGULATORS PERSPECTIVE ON PERSONAL DATA AND PRIVACY OF USERS.

SPEECH DELIVERED BY PROF. UMAR G. DANBATTA EXECUTIVE VICE CHAIRMAN NIGERIAN COMMUNICATIONS COMMISSION (NCC) AT KANO INTERNET FREEDOM FORUM (KIFREF). ORGANIZED BY CENTRE FOR INFORMATION TECHNOLOGY AND DEVELOPMENT (CITAD)

INTRODUCTION.

Technological advances give insights into what constitutes consumer's needs, wants and behaviors. Businesses collect data in order to deliver personalized services to meet consumers' yearnings and behaviors. However, as technologies become more intelligent and intrusive, there is an increasingly higher risk of consumer's personal data being misused or compromised.

The Federal Government through some of its agencies - Nigerian Communications Commission (NCC), National Identity Management Commission (NIMC), Central Bank of Nigeria, Federal Road Safety Corps (FRSC), INEC, FIRS, etc. had implemented various initiatives that warranted the collection of citizens' personal data. Such initiatives include the SIM card registration, National Identity Card registration, New Vehicle License regime, BVN, Voter's Card, Tax Identification Number (TIN) and a host of many others.

Developments in the telecommunications industry have also led to a large growth in various telecommunication services and a corresponding rise in the number of subscribers.

The Federal Government's efforts to increase Internet penetration via the deployment of broadband and the move for the adoption of cloud services makes it crucial that the security of citizens' personal data and privacy issues be critically looked into.

It is therefore imperative that appropriate enabling laws need to be enacted side by side with these initiatives, technologies, and services, while at the same time efforts should be geared towards trimming and harmonizing the warehousing of personal data in order to enhance security and accountability.

Some countries have put in place laws to protect their citizens' data and privacy, while some are in process of putting finishing touches to theirs. These laws will be used by these countries and

they will affect citizens of other countries, irrespective of whether or not there exists one within their own countries.

With appropriate enabling laws, infringements on citizens' rights and privacy as it relates to personal data can be curtailed.

The Main Issues at Stake:

The major concerns, which are by no means exhaustive, can be listed as follows:-

- Concern about possible breaches to collected personal data such as - unauthorized access, misuse, identity theft, etc.
- Inconveniences faced by citizens in having to go to different organizations to register and provide the **same** set of data.
- The need for agencies and organizations to provide convincing assurances that these personal data are hosted or kept in secure locations.
- Abuse of users' privacy via **unsolicited messages or calls** in the form of advertisements and the likes.

Possible Solutions to Address these Concerns.

There are some existing policy documents that may need to be revisited / reviewed:-

- The National Information Technology Policy, which stressed the need for the enactment of a **Data Protection Act.**
- The National Data Protection Bill which is yet to be passed, is itself full of inconsistencies and omission of certain vital aspects and does not fully address the main concerns.
- The Industry has established a "***Do Not Disturb"*** registry via the service providers; Consumers have the right to demand that certain calls/messages do not get to them.

From the Commission's Perspectives, the following are proffered as directions:

- It is necessary to put in place a deliberate policy/mechanism (or review related existing ones), that will specifically focus on protection of citizens data and privacy.

- An Inter-agency and Multi-stakeholder working group should be established. This will ensure that the various views and opinions are taken into consideration in the development of the necessary framework for data protection.

- Data **aggregation and harmonization** would need to be considered; as this will ensure that a citizen's data captured by one organization is available for use by any other authorized agency that requires same records, without having the citizen go through the process all over.

- The process of harmonization should include a clear definition and identification of what is considered personal data.

- Generally, the data protection framework should take the following into consideration :-
  - ✓ Collection, Classification and processing of Citizens' data
  - ✓ Storage and Retention of Citizens' data.
  - ✓ Access and Use of Citizens' data.
  - ✓ Transfer of Citizens' data.
  - ✓ Disclosure and Publication of Citizens' data
  - ✓ Aggregation of citizens' data.
  - ✓ Penalties for clearly spelt out breaches.
  - ✓ Etc.

Conclusion.

The development of the framework proffered above, should be focused towards building the much needed trust between users / citizens and the agency (or agencies) that warehouse the aggregated information and data.

The equity considerations and the nation's reputation should also be paramount.

In the global context, this would help cross-border transfers of information and strengthen Nigeria's position as a trusted business hub.

Thank you.
October 22nd, 2015