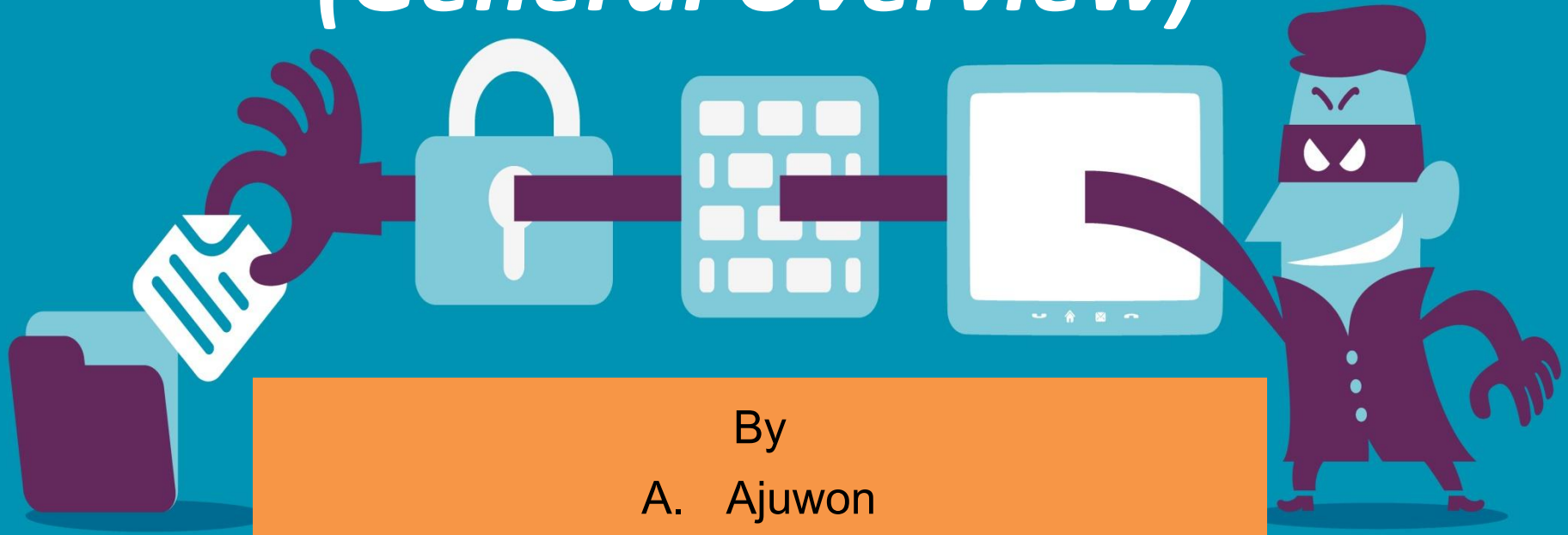


Why Data Protection is important and Current Trends *(General Overview)*



By
A. Ajuwon
*African Academic Network on
Internet Policy*

The African Academic Network on Internet Policy (ANNOIP)

A Pan-African think tank on internet policy leveraging on the rigour of localised research and its application to drive the growth of the African digital economy. It is a network for interdisciplinary scholarly engagement and discussion on the state of the internet, related policies and regulatory regime in Africa.

The Network has 6 thematic areas of focus and they are:

- ☐ Economic Diversification (Innovation, Entrepreneurship and start-ups)
- ☐ Access (Infrastructure and Finance)
- ☐ Content (Intellectual Property, Piracy, Intermediaries and Copyright)
- ☐ Privacy and Security
- ☐ Knowledge and Capacity Building.
- ☐ Human Rights



The African Academic Network on Internet Policy (ANNOIP)

❑ The African Academic Network on Internet Policy (ANNOIP) has Data Protection and Privacy as a thematic area of focus and the first seminar was on Data Protection in Nigeria. Present at the seminar were stakeholders, students, academics and professionals.

❑ Working groups were created so participants can discuss issues like: Data privacy and Protection as an Enabler of Innovation, Data Protection as an ICT issue, the groups also discussed on how to make members of the society aware of data protection and steps to take.



WHAT IS DATA PROTECTION?

"Personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be recognized, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.





- Every Nigerian has a right to privacy because of Section 37 of the 1999 constitution.
- “ *The **PRIVACY** of citizens, their homes, correspondence, telephone conversations and telegraphic communications s hereby guaranteed and protected*”
- The Constitution is the most supreme law in Nigeria. The provision is not sufficient with the rapid manner in which technology evolves.

PROTECTION

DATA

PRIVACY

- Nigeria doesn't have a Data Protection Law. There are industry specific laws/rules but the most comprehensive NITDA Guidelines is still a draft.
- According to a 2017 report, 97.2 million Nigerians are connected to the internet.
- How many Nigerians understand the concept called "Privacy" ?

Examples of the type of personal data collected in Nigeria

Offline	Online
<ul style="list-style-type: none">● Name● Fingerprints● Facial photographs● Residential address● Telephone number● Health information	<ul style="list-style-type: none">● Name● Email address● IP address● Clickstream data● Telephone number● Location information● Sexual orientation● State of Origin● Birthdates

Some organizations that collect personal data in Nigeria

Offline	Online
<ul style="list-style-type: none">● NIMC● INEC● Nig. Immigration● VIO/ FRSC● Banks and financial institutions● Hospitals/HMOs	<ul style="list-style-type: none">● Google● Youtube● Facebook● Twitter● Whatsapp● Trucaller● ISPs

5 STAGES OF DATA PRIVACY GRIEF

DOESN'T
AFFECT ME.
I DON'T
EVEN USE
FACEBOOK
THAT MUCH.



TOM
FISH
BURNE

DENIAL

WHOA!
HOW DO
THEY HAVE
5GB OF
DATA ON
ME?

#DELETE



ANGER

IS IT WORTH
LETTING
COMPANIES
COLLECT
SO MUCH
OF MY DATA
FOR FREE
SERVICES?



BARGAINING

FACEBOOK
IS ONLY THE
TIP OF THE
ICEBERG.



DEPRESSION

THERE'S A
SPECIAL ON
MINT CHIP
ICE CREAM
THAT MIGHT
CHEER YOU
UP.



ACCEPTANCE

CASE STUDY

FACEBOOK & CAMBRIDGE ANALYTICA

2013: Cambridge academic created an app called “This Your Digital Life”. The app was used by FB users, their data and their FB friends were harvested.

2014: FB made new rules to limit developers access to user data. The rules were meant to prevent third party like “TYDL” from accessing your friends data without their permission. The creator of TYDL didn’t delete the data he had acquired.

2015: Cambridge Analytica “**a political consulting firm/company that combines data mining, data brokerage and analysis with strategic communication for the electoral process**”. CA was employed by Fmr. US Presidential candidate Ted Cruz to win the election.

2016: Cambridge Analytical was heavily invested in Trump’s election and they influenced his winning.

2018: It was revealed by a whistleblower, one of the creators of Cambridge Analytica that they had the data of over 57 million Facebook users. The world is alert.

8 PRINCIPLES OF DATA PROTECTION

Fair and Lawful

Adequate to needs

Specific for its purpose

Accurate and up to date

Not kept longer than needed

Take into account People's right

Kept safe and secure

Shouldn't be transferred internationally without adequate protection.

GDPR FOR BEGINNERS



KEY DATA PROTECTION REQUIREMENTS

for GDPR compliance

ARTICLE 15

Grants EU citizens the **RIGHT OF ACCESS** which requires companies to detail what personal data is being processed and how upon request

ARTICLE 17

Grants EU citizens the **RIGHT TO BE FORGOTTEN AND TO DATA ERASURE** which requires companies to stop processing and delete personal data upon request

ARTICLE 20

Grants EU citizens the **RIGHT TO DATA PORTABILITY** to enable citizens to transfer personal data between companies upon request

ARTICLES 25 & 32

Require companies to implement **REASONABLE DATA PROTECTION MEASURES** to protect EU citizens' personal data and privacy by design

ARTICLES 33 & 34

Require companies to **REPORT DATA BREACHES TO SUPERVISORY AUTHORITIES AND INDIVIDUALS** affected by a breach within 72 hours

ARTICLE 35

Requires companies to perform **DATA PROTECTION IMPACT ASSESSMENTS** to identify risks to EU citizen data and outline measures to ensure those risks are addressed

ARTICLE 37

Requires certain companies to **APPOINT DATA PROTECTION OFFICERS** to oversee data security strategy and GDPR compliance

Penalties for GDPR

NON-COMPLIANCE

€20 MILLION

or

4%

 OF GLOBAL ANNUAL
TURNOVER

ARTICLE
83

OUTLINES FINES FOR
NON-COMPLIANCE

which can be up to
whatever is greater:



52% of companies BELIEVE THAT **THEY WILL BE FINED** FOR NON-COMPLIANCE with GDPR⁵

How can

COMPANIES PREPARE FOR GDPR?



Hire a data
protection
officer



Create a data
protection
plan



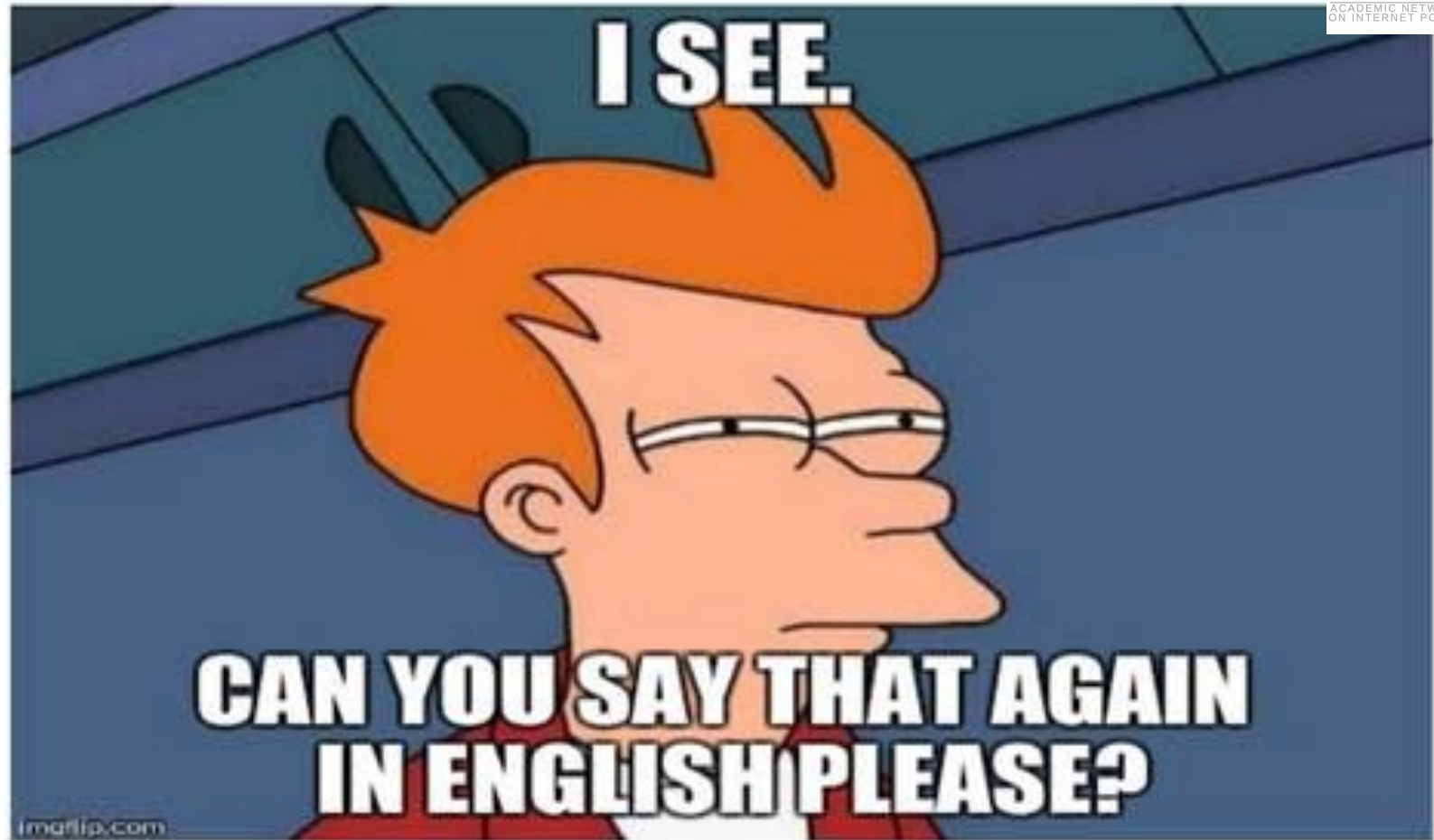
Conduct a risk
assessment to
identify EU citizen
data and where
it is at risk



Implement security
measures to mitigate
risk and comply with
GDPR requirements



Assess on a
regular basis
for continuous
improvement



GDPR makes it clear that EU Citizens **own** their data and can **decide** how their data is used.

What you should know

**May 25th
2018**

Enforcement
date

**4% of
annual
global
turnover or
€20M**

Fines for Non
Compliance

EU citizens

Who it protects
(Data Subjects)

Personal data protection ecosystem Actors

- **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 or data processor



Personal data protection ecosystem in Nigeria: Interactions

- Data subject provides personal data to the data controller
- Data controller provides personal data to the data processor
- Data subject provides personal data to the data processor for processing on behalf of the data controller
- Data controller provides the data subject upon request made by the data subject
- Data processor provides personal data to the data subject as directed by data controller
- Data controller provides personal data to a third-party

HOW TO PROTECT YOUR DATA ONLINE

**Back up your
data**

**Always use
anti-malware**

**Set system to
update app
automatically**

**Turn off you
computer when
not in use**

**Password your
hotspot/internet
device**

**Don't store
passwords on
phone/laptop**

**Switch off the
internet when
not in use**

**Always disable
Bluetooth when
not in use**

**Lock your
phone**

**Read privacy
setting**

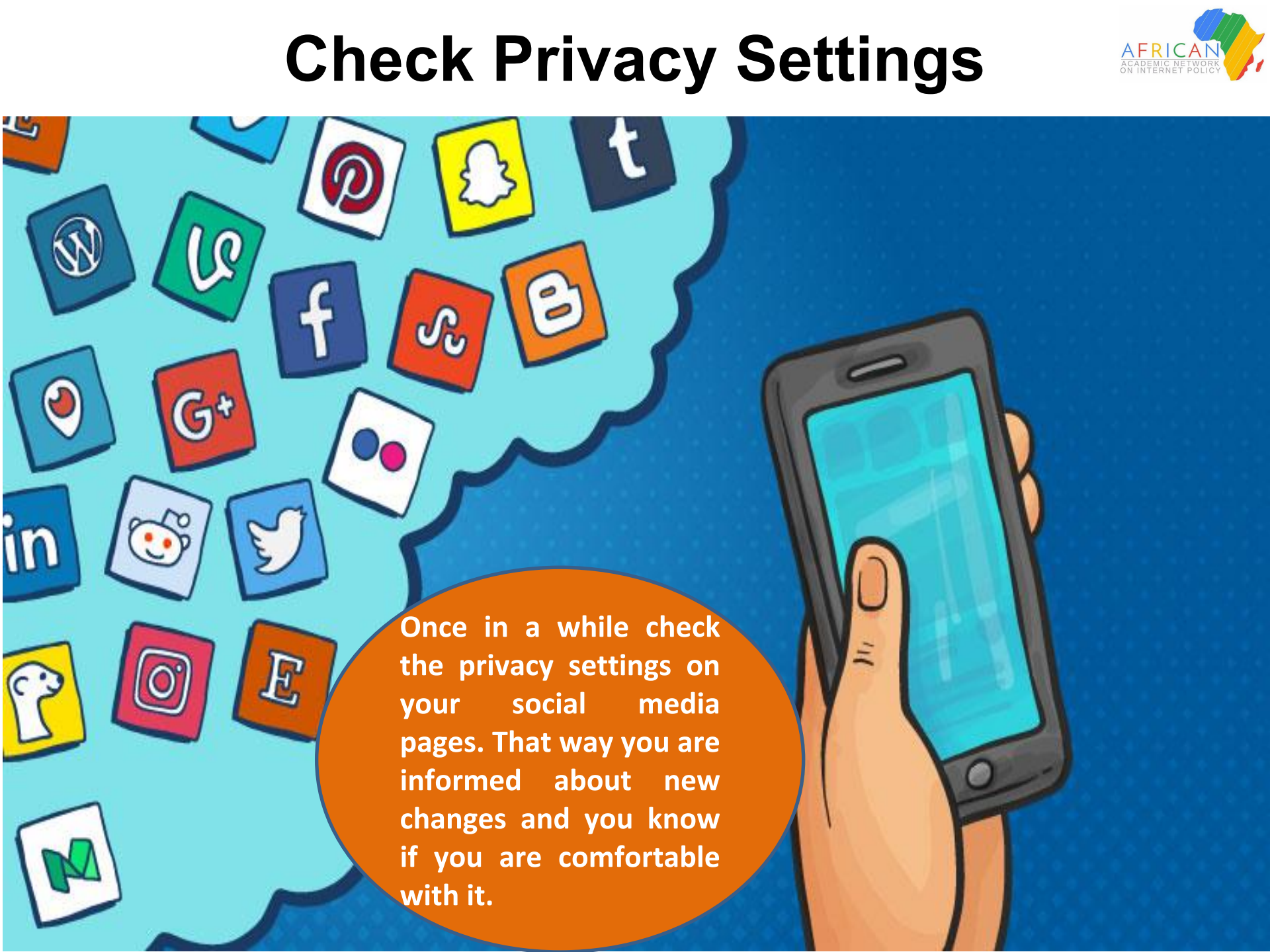
**Be Weary of
PHISHING**

**Be mindful of
the apps you
install**

YOUR DIGITAL FOOTPRINTS

- **Digital Footprint** is an *individual's unique set of digital activities , actions and communications that leave a data trace on the internet or on a computer or other digital device and can identify the particular user or device.*
- Two types of Digital Footprint: Passive and Active Digital Footprint
- **Passive:** Footprints you leave without knowing.
- **Active:** Footprints you leave when you make deliberate choices on the internet.

Check Privacy Settings

An illustration featuring a collection of various social media icons (including WhatsApp, Telegram, Facebook, Twitter, Instagram, and others) floating in a light blue cloud-like shape on the left. On the right, a hand is shown holding a black smartphone with a blue screen. In the center, an orange oval contains text.

Once in a while check the privacy settings on your social media pages. That way you are informed about new changes and you know if you are comfortable with it.

Facebook Privacy Setting

Settings

Logout

Search



Account Settings



Privacy Settings

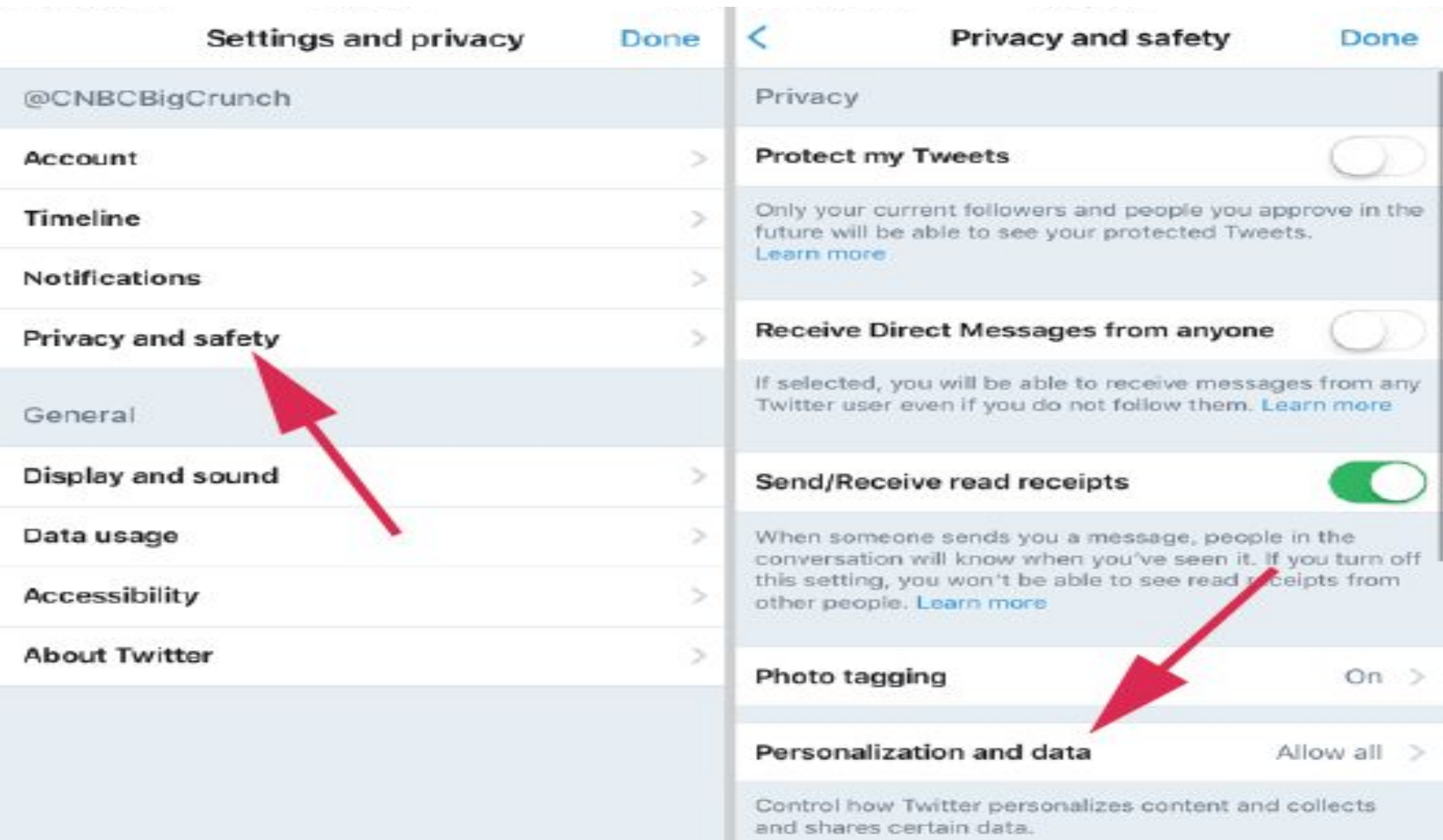


Application Settings



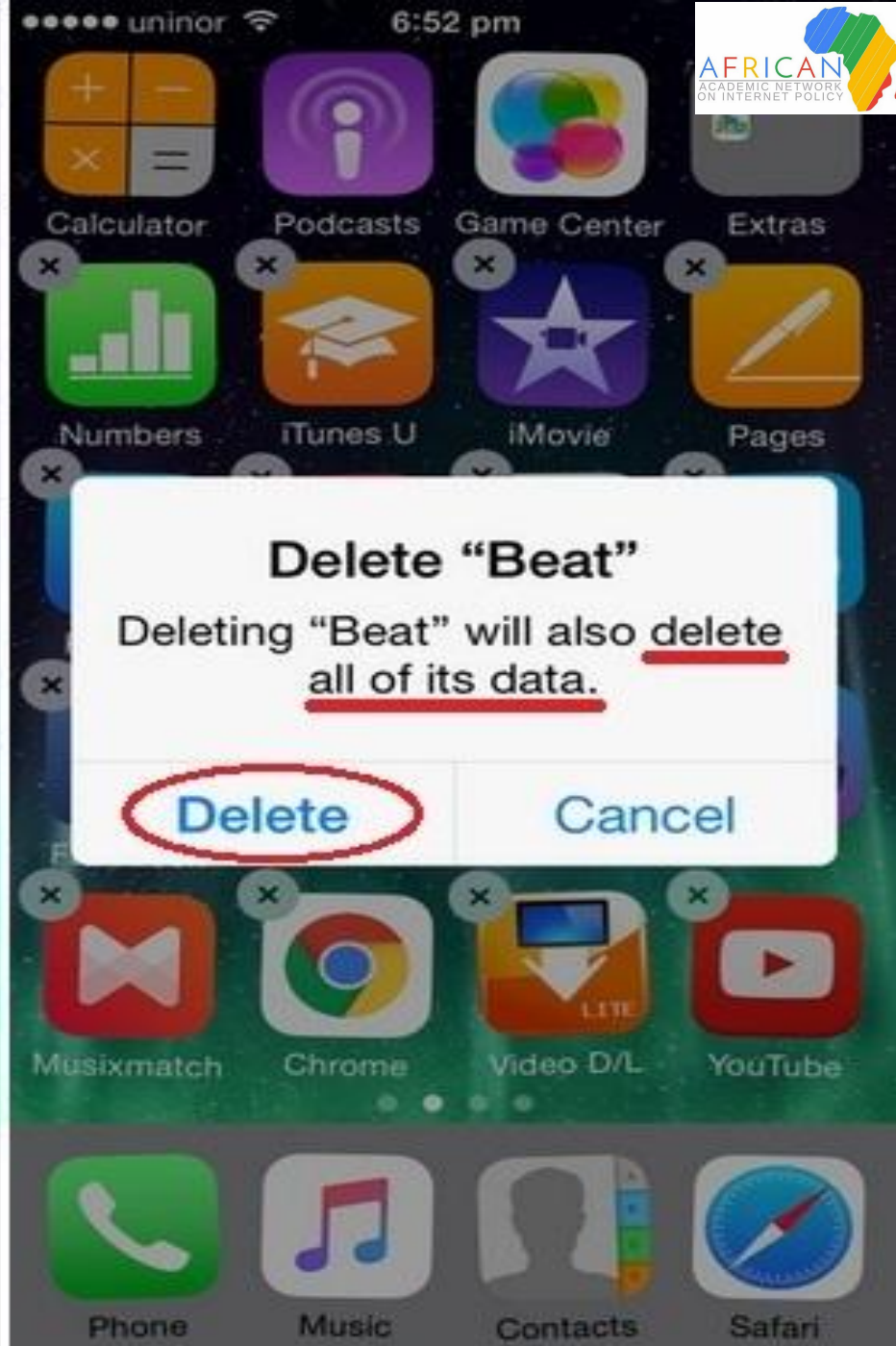
Help

TWITTER PRIVACY SETTING



DELETE UNUSED APPS

- Any application that you are not using on your phone and laptop should be deleted. You free up space on your phone and one less company collecting your information.



We ALL leave a digital footprint

Once it's on-line it's
virtually impossible
to scrub out

.. and the data
on you will follow
you around for life



The Nigerian Context of Data Protection

- ❑ The Constitution does not have a provision that adequately encapsulates data protection of citizens specifically as a stand-alone without strict rules of engagement.
- ❑ It is trite knowledge that data plays an increasingly important role as the currency of Nigeria's emerging digital economy, hence, the need for data privacy and information protection



Little to no transparency around the processing of personal data and limited information on its use and storage

Absence of rights to consent to or opt out of data collection

Use of personal data is not compatible with the purpose for which it was collected.

Industry specific laws wouldn't have the same weight as a comprehensive data protection law

Issues of identity theft and related fraudulent activities due to the absence of a credible data protection law

Grave exposure of Children to privacy risks online and lack of legal capacity to give valid consent

POLICY RECOMMENDATION

The use of personal data must be in accordance with the purpose for which it was collected

The consent of the individuals must be obtained prior to collecting his/her personal data

The consent of the individuals must be obtained prior to collecting his/her personal data

Enact a Data protection Act with principles consistent with those contained in the African Union Convention on Data Protection and /or the EU's (GDPR).

To enact a child Online Privacy Protections provisions into the Child's Right Act.

Amend the National Identity Management Commission Act to contain robust data protection principles and expand powers of NIMC to function as a data protection authority

CONCLUSION

A close-up, slightly angled shot of a smartphone screen resting on a light-colored, textured surface. The screen displays a blue and yellow interface. The word 'SECURITY' is visible at the top. Below it, there is a toggle switch labeled 'OFF'. The phone is black with a silver bezel.

In conclusion, the AANOIP is focused on creating more awareness and the partnership with the Ibadan School of Government and Public Policy to ensure that the discussions and ideas generated for the availability of a standard data protection and privacy law comes into existence.

Thank
you!