



## WHO CAN YOU TRUST?

-  
GSMA Mobile 360  
Kigali July 2019

-  
Daddy Mukadi  
CRO Airtel Africa



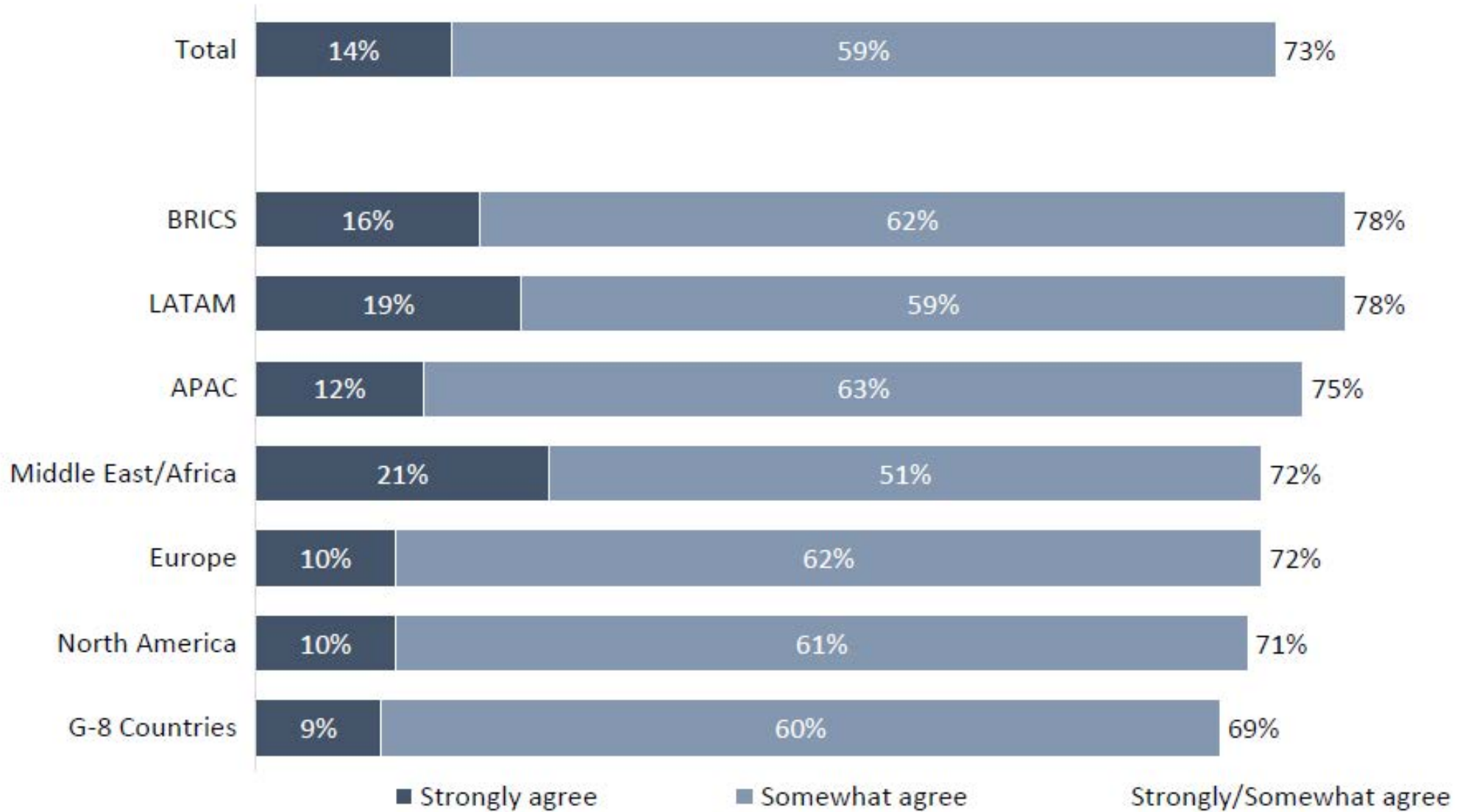
### CHALLENGES:

- **National Security** – government have a genuine need to protect its citizen
- **Personal safety for all** – (Location data can pin point where an individual is with precision)
- **Safeguards regarding data on children?** (how do we differentiate the data of minors for different treatment)
- **Consent of the owner of the data?** (Are the long T& C acceptable and sufficiently constitute consent)
- **Is the data collected legitimately?**
- **Location - Where is the collected data anyway?**
- **Security of financial data and systems** (records of transactions and logs)
- **Health related Data exposed**
- **Protection against Cyber crimes**



# Trust in Internet

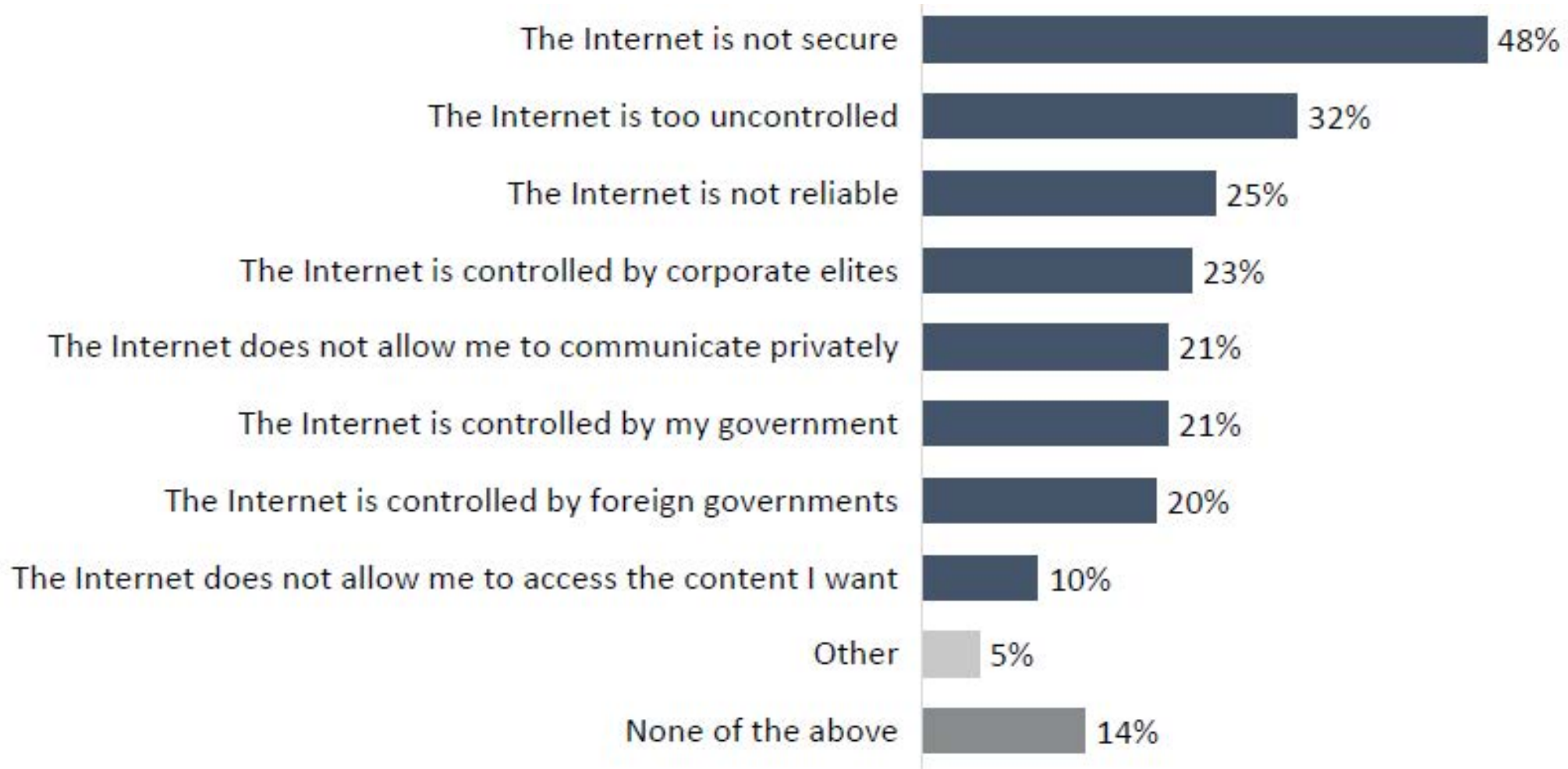
## Overall, I trust the Internet— By Regional Economy



Source UN : Global survey on Internet Security 2018

## Question around Trust in Internet : Reasons

People are generally more inclined to distrust internet for a variety of reasons



### The Importance Of Transparency

- Businesses that collect and monetize consumer data need to be transparent with consumers about their behavior.
- In fact - Current privacy concerns often revolve around data that has been collected without well-defined and transparent terms of use.
- When collecting Data, Companies should use clear, concise language rather than tens of pages of legal terms
- Companies to ensure that consumers understand how information is collected, processed, stored, and potentially shared with other parties.
- Consumers MUST be allowed to evaluate the costs and benefits of a transaction by applying their own personal level of concern for data privacy.
- A business that collects consumer data should make it apparent to consumers that their data are being managed responsibly, securely, and within industry-specific guidelines



# Role of Government

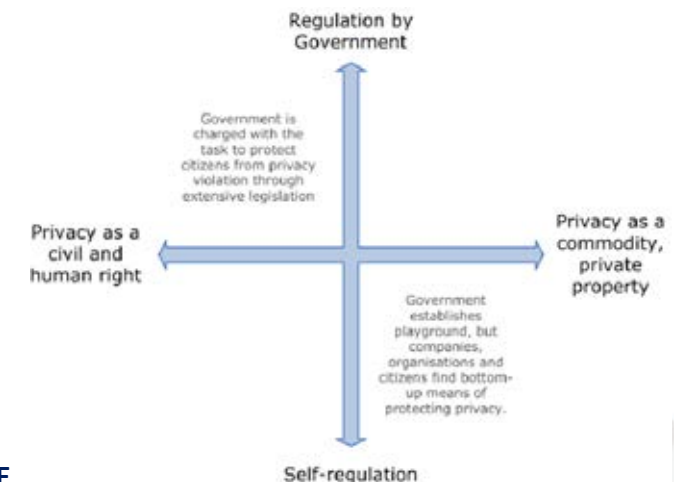
- ❑ Government to ensure Coordinated effort with Private Sector / Consumers to come up with the right framework.
- ❑ Government to Strike the right balance between **PRIVACY, INNOVATION, SAFETY AND SECURITY**.
- ❑ **Some key top issues to be addressed:**

- *Customer rights notice that their Data is being collected*
- *Obtain customer consent for collection of their data*
- *Measures for ensuring data security*
- *Customer right to access their personal data and to request for correction*
- *Obligation on private enterprise to ensure accurate data and protect its integrity*
- *Rules for data retention and destruction*
- *Customer right to be notified when a data breach occurs*

## ❑ Big Challenge For Governments :

SOME COMPANIES WHO ACTUALLY MONETISE DATA ARE DIFFICULT TO BE HELD ACCOUNTABLE GIVEN THEIR NATURE (OFF- SHORE) .....

.....**QUID** ON HOW TO HOLD THEM ACCOUNTABLE ? A MUCH BIGGER DEBATE ...DATA SOVEREIGNTY ....etc ...



A person wearing a dark hoodie is seen from behind, looking at a large digital display. The display is filled with binary code (0s and 1s) in various colors (blue, green, white). In the center of the display, the word "HACKED" is written in large, bold, red letters. A black oval with the text "THANK YOU" in white is overlaid on the top part of the image.

THANK YOU

**HACKED**