2018 ANNUAL CONFERENCE OF THE AFRICAN BAR ASSOCIATION CONFERENCE
NAIROBI, KENYA
22 JULY 2018 – 27 JULY 2018

"Africa's Socio-Economic and Political Future: The African Union's Agenda 2063 in Perspective"

Metadata Exposure in Africa

Intro:

What is metadata? Metadata is "data about data" – sets of information providing information about other data. The purpose of this kind of data is that it helps organize information in an easy and accessible manner. Originally, metadata was used in libraries in the form of card catalogs. Since the 1980s, metadata began to digitalize as the digital format prevailed. Currently, metadata is almost exclusively in the form of digital information. This information is extracted through the various programs users download, use and access on their phones, computers, televisions etc.

Applications such as Google, Facebook, Twitter, WhatsApp, Snapchat etc. are widely used social networks that can provide information on their users. The metadata can be collected from a range of pictures, videos, links shared, to likes and comments made as well as locations checked-into. Based on this, it is possible to develop profiles on individual users to discover the frequency and pattern of users' activity. This is not limited to one application, but functions also in conjunction with other websites and programs.

Since metadata is largely available through the internet, this also means that national governments are in possession of large amounts of the metadata on their own people as well as people from other parts of the world.

Issues:

This is problematic for multiple reasons. The possession of this kind of information is ultimately an issue of national security. It is also a threat to privacy. The extent to which the possession of metadata is problematic was exposed by former CIA employee Edward Snowden in 2013. Recently, Cambridge Analytica has further shown the world how the possession of such

data can allow the manipulation of voters during an election campaign or referendum.[1] Cambridge Analytica paid 32 000 Facebook users to take personality tests the results of which later translated into approx. 87 million profiles. This enabled the creation of Algorithms combining data with voter records to allow personalized advertisement for each Facebook user. The issue, here, mainly concerned the data collected from those individuals who did not give permission of access to their account information. It is thus evident that the issue at hand is no longer one limited to one's right to privacy but rather a matter of national security. For instance, when this information is used to manipulate an election by another state.

This is possible through various channels depending on the services each Application provides and the type of information they accordingly obtain. Google collects information specific to individual users on what services are used and how these are used. Phone numbers or device identifiers are linked to the account and used accordingly in data collection. This information is used for surveillance programs to create user profiles, especially used by the US military in drone operations.

YouTube, another internet success - established by Google in 2005, has grown into the largest video sharing website on the internet. YouTube facilitates video-sharing but also provides no control for the content that is shared (e.g. violence).

WhatsApp, moreover, collects all conversations and contacts from all users. This helps recognize the influential and connected individuals. These users can then be tracked through call logs, messages and especially location. In combination with data from Truecaller, for example, phone numbers can also be easily identifiable.

Another feature that gives away substantial and critical data is the enabled location on all devices nowadays. Facebook is among the providers that use users' location to suggest friends, for instance as 'People you may know'. The social network admitted to doing so, claiming to combine data with other factors such as work, education or mutual friends, to offer more people a user might want to connect with. This data collectively can easily map the entire network of any given individual, identifying family members, co-workers, degree of intimacy with friends etc.

In comparison to the rest of the world, Internet penetration in Africa represents approximately 35%. The average internet penetration worldwide is around 55%. Between 2000 and 2017 the internet growth in Africa translates to 9942%. This means that the African continent is increasingly at risk from potential outside manipulation.

Africa, in this respect, has a blind spot compared to the rest of the world. As users continuously expand in Africa, metadata assists in better mapping of complex societies and countries. Knowledge of ideological demographics, political debates and platforms, religious beliefs are all tools for political as well as economic dominance.

[1] Bowcott, Owen, and Alex Hern. "Facebook and Cambridge Analytica Face Class Action Lawsuit." *The Guardian*, Guardian News and Media.

For that reason, China has created its equivalent Google and Facebook providers to secure its network and gain control over its own information. The European Union similarly has adjusted its General Data Protection Regulation (GDPR) after the events of Cambridge Analytica. The GDPR is a regulation that requires companies to protect the personal data and privacy of residents of EU countries. It strengthens the rights that individuals have regarding personal data relating to them and seeks to unify data protection laws across Europe, regardless of where that data is processed.
That way, the release of information originating within the EU to exit the Union without permission is prohibited. This has called for Google, Facebook etc. to establish offices on EU ground. The EU, thus, gains autonomy over information emanating from within its borders.

Solution:

What Egypt (Egyptian Satellite Operator) can offer:

1. A secure (closed) network within the African continent
    a. 3 cables in Egypt redundancy secured

The role of satellite operators in these regards could be more or less useful in linking the local backbone with the more advanced Egyptian backbone, where more security measures and higher standards are applied, reducing significantly the local data access. Such claim needs to be well coordinated with Egyptian local authorities, as somehow this could be logistically increasing the burdens of surveillance and monitoring. Satellites could be used to secure the inter-African state communication, i.e. if (by a way or another) Africa is isolated from the rest of the world, still the communication between the African states shall be possible as the hubs and satellites shall be all Africans and physically located within the African soil.

2. Africa-wide Regulations for Google/Facebook/LinkedIn restricting the emanation of African metadata outwards (similar to EU's GDPR)

Prior using the site services or applications, a mandatory request of consent for collecting, sharing, and processing data from users is requested. If it is not given, the user shall not be able to use the service or application, taking into consideration that the means of use of such data are never announced.
Until recently, all Facebook users outside U.S. and Canada have been governed by terms of service agreed with the company's international headquarters in Ireland. Accordingly, all data that are processed in Ireland should be treated according to GDPR.
To avoid being complied with this regulation, Facebook changed its terms of service so users in other parts of the world like Africa, Asia, and Latin America under Facebook Inc. in Menlo Park, rather than be subject to the US laws.

African nations, therefore, ought to formalize a law that to be applied all over the continent seeking to protect and organize the use of such applications in Africa. The required technical expertise should be sought and exploited from within the continent to limit the use of data within the continent. That way, all regulators in Africa would get together to make way for the "Internet" Companies to introduce their servers to be in Africa.

3. Pan-African Application to replace above mentioned Applications and websites – tailored to each country
    a. Utility
    b. Easy to use
    c. Accessible
    d. Price: free.

This is to propose a development of an African application. Such a development would be appealing to African users. The Chinese and North Korean model suggest the possibility of creating an African search engine, African social networking applications. These should be tailored in a way to meet Pan-African needs. Such applications should fulfill some basic elements: Utility, Accessibility, perceived ease of use and cost.
The development of such applications will increase the need of African secured internet which could be obtained through satellite operator (Egypt for Example) and would increase the demand for more capacities.

Potential barriers:

a) Existing Applications: Facebook, Instagram, Snapchat, WhatsApp, YouTube, LinkedIn, Truecaller etc.
b) Cultural barriers and preferences
c) Diverse populations (different usage)
    a. communication purposes
    b. Work/networking
    c. Meeting new people
    d. Educational purpose

To overcome these obstacles, accurate and thorough research ought to be done on demographic data about African internet users as well as the age segmentation of users. This information will be of extreme importance in shaping the general concept of such applications.

Conclusion:

African Metadata is well exposed with zero control over it. This lack of control may be a loophole in the national security of the African continent. This is why a call for a Pan-African action and monitoring is necessary.

For more information, submission of abstract and registration details, please go to the official website of the Conference: www.afribar.org

To get in touch with the conference organizing committee, please email: bhi@id.com.eg