

2019 ANNUAL RETREAT AND CONFERENCE OF ACAEBIN

DATA SECURITY AND PRIVACY- GLOBAL
PERSPECTIVES

PRESENTED BY ROTIMI OGUNYEMI
ICT ATTORNEY



The Economist

MAY 6TH-12TH 2017

- Crunch time in France
- Ten years on: banking after the crisis
- South Korea's unfinished revolution
- Biology, but without the cells

The world's most valuable resource

DATA

The world's most valuable resource is no longer oil, but data. Land was the raw material of the agricultural age, Iron was the raw material of the Industrial age, Data is the raw material of the Information age. Every new and emerging technology depend on data

INFORMATION ASSETS

Information or “**Data**” has become a critical resource upon which the prosperity of individuals and society depends. A connected society necessarily churns out vast amounts of useful data making such data extremely valuable asset

Information assets: When talking about valuable data we use the term ‘information assets’



BAYOOGUNYEMI & CO

ICT ATTORNEYS, ADVOCATES & CONSULTANTS

Privacy:The right of individuals to be left alone;
Free from surveillance from other individuals and
organisations, including the State

Information Privacy:(Is a subset of Privacy)

The right (claim) of individuals to control one's own
information and the claim that some information
should not be collected at all. It includes the right
(claim) by individuals of control of information
collected about them by other individuals,
organisations or the state.

PRIVACY AS A HUMAN RIGHT

PRIVACY

- Limitations on what Personal information governments or private institutions can collect and use is a foundation for democracy
- As Power and wealth is being increasingly determined by Data and knowledge as core assets, the risks of abuse and criminal exploitation heightens



DATA SECURITY

The growth of the information society is accompanied by new and serious threats. Essential services such as water and electricity are increasingly dependant on ICTs. Financial services, health services and commercial activities all depend on ICTs. These developments have made ICTs an attractive target for civil and criminal violations



Physical Security



Secured Connections



Cookies

DATA SECURITY & PRIVACY



Network Security



Authentication



Malware

At the end of the day, all of **Data Security and Privacy** boils down to **TRUST;**

Trust of People, software, Platforms, Private organisation and governments



Threats to Data Security & Privacy

GOVERNMENTS AND STATE ACTORS

- Privacy is increasing difficult to protect as mobile behaviour, profiles, and transactions of consumers are routinely available to governments and state actors
- In June 2013, Edward Snowden former NSA employee revealed that the NSA had after the events of September 11 2011 been collecting massive phone and internet data by wiretaps and other means of US and non-citizens including world leaders, all over the world




Government Invasion of Privacy

Striking a balance between security and freedoms is at the heart of the privacy debate

Various US Statutes strengthen the ability of US law enforcement authorities to monitor internet users without their knowledge

Others compel Internet Firms to disclose their privacy and data use policies in plain language, to Inform consumers about what Data is collected and to Provide consumers with greater control over the use of their personal data

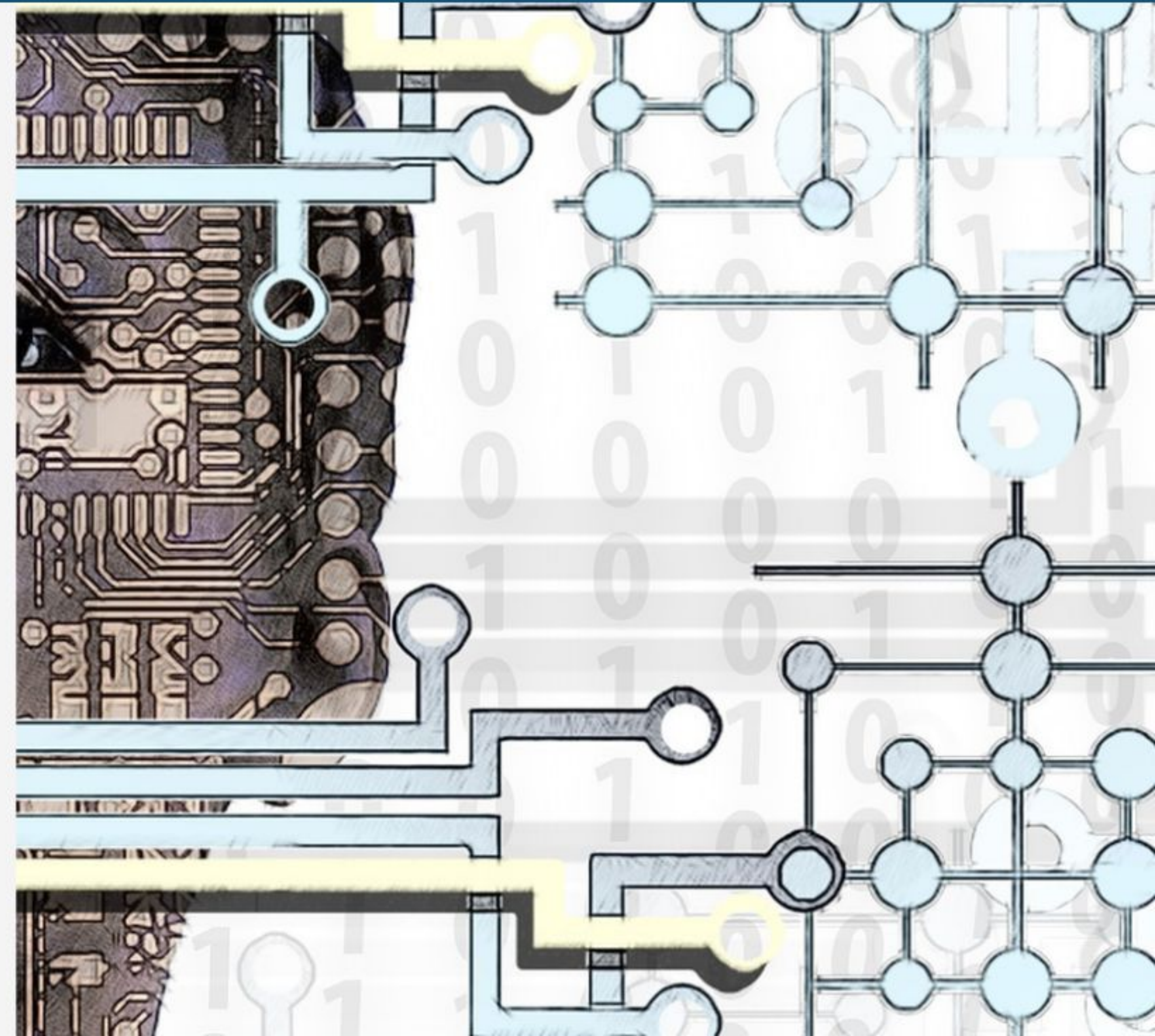


Governments and the **Private sector** pose a threat to privacy as both can leverage **Deep Packet Inspection**- A *technology for capturing all internet traffic at ISP level*

Threats to Data Security & Privacy

PRIVATE SECTOR

- Collection of information by commercial websites and the use of such collected data
- Proliferation of tracking technologies, smart phones fitted with GPS & sensors, expansion of storage and analytical capabilities have resulted in torrents of data: Known as Big Data - pouring into marketing and law enforcement databases





THREATS TO PRIVACY: E-COMMERCE

- User Information Collected on E-Commerce sites
- **Personal Identifiable Information** - Being information that can be used to identify, locate or contact customers
- **Anonymous Information** - Demographic and behavioural information such as age, occupation, income

Private Sector Invasion of Privacy - Mobile

Smart Phone apps tap users information

Mobile applications track users' location - Collecting data on places visited in real-time and collecting detailed logs of their phone calls (call data)

Apple, Facebook and Google collect personal location and behaviour data and share these with marketers and sometimes government

Facial recognition technology - perhaps a more concerning issue



Private Sector Invasion of Privacy - *Mobile&Location*

Smartphone Manufacturers - IOS and Android Apps have capabilities of funnelling location information, address books and photos to mobile advertisers

Apple (for instance) can target ads based on the apps that a person has downloaded

In 2014, a US Supreme Court ruled that the Police needed a warrant to search an individual's cell phone for information

Using a person's cell phone to establish identity or location does not require a warrant





THREATS TO PRIVACY: ONLINE ADVERTISERS

- **Online Advertising Networks** have the capabilities to precisely track consumer purchases and all browsing behaviour online
- Some have created spyware that's placed on consumers devices and reports back to advertisers servers on all consumers internet use: and it displays advertising on consumer's device
- Google's search algorithms allows advertisers using **Google's Ad words** to target advertisement to consumers based on consumers' search histories and profiles

Threats to Privacy - *Online Advertisers*

Googles uses behavioural targeting to help it display more relevant ads based on keywords

Google's gmail, a free email service, offers a powerful interface and gigabytes of free storage. In return, google's computers read all incoming and outgoing mail and can therefore place "relevant" advertisement at the margins of the mails. Google profiles its users based on the content of their email



Threats to Privacy - *Online Networks*

Networks argue that web profiling is good for everyone, as targeted ads reduces nuisance value for consumers and reduces waste for advertisers

Cookies placed by ad networks can be persistent as they could be active for a very long time tracking user activities across thousands of websites and creating web profiles

More disturbing if and when anonymous information collected over time is linked to **user's personal identifiable information**, whether online or offline



THREATS TO PRIVACY- SEARCH ENGINES

When you use a search engine, the IP address of your device is logged and cookies are placed on your browser to record the search terms of the current session, time of visit, and links you actually chose



Threats to Privacy - Search Engines

User logged information is stored in a database where it can be related to previous searches and other **personal identifiers** that the search engine may have gleaned from previous searches

Search engines' database provide a comprehensive picture of a person's intentions and actions on the internet





<https://google.com/myactivity>

Threats to Privacy - Social Networks

Facial recognition technology makes it possible for algorithms to “recognise” a user in a photo and such a one can be potentially “tagged” without their consent. The software is used to automatically suggest name tags for persons in a photograph

Facebook Privacy Policies allows it to share users data with advertisers to deliver targeted ads to users all over the web

Individuals may have volunteered their information to social networks, but they want to be in control of how such information is used



F A C E B O O K ' S C A M B R I D G E A N A L Y T I C A S C A N D A L

Cambridge Analytica's improper mining and abuse of personal data of Tens of millions of facebook users for political purposes was perhaps the most recent example of massive privacy violations on a digital platform. Facebook was fined by the UK Information Commissioner's Office for failing to take appropriate technical and organisational measures to prevent the data from falling into the wrong hands

UK's Information Commissioner's Office (ICO)

"The ICO's investigation found that between 2007 and 2014, Facebook processed the personal information of users unfairly by allowing application developers access to their information without sufficiently clear and informed consent, and allowing access even if users had not downloaded the app, but were simply 'friends' with people who had.... Facebook also failed to make suitable checks on apps and developers using its platform"



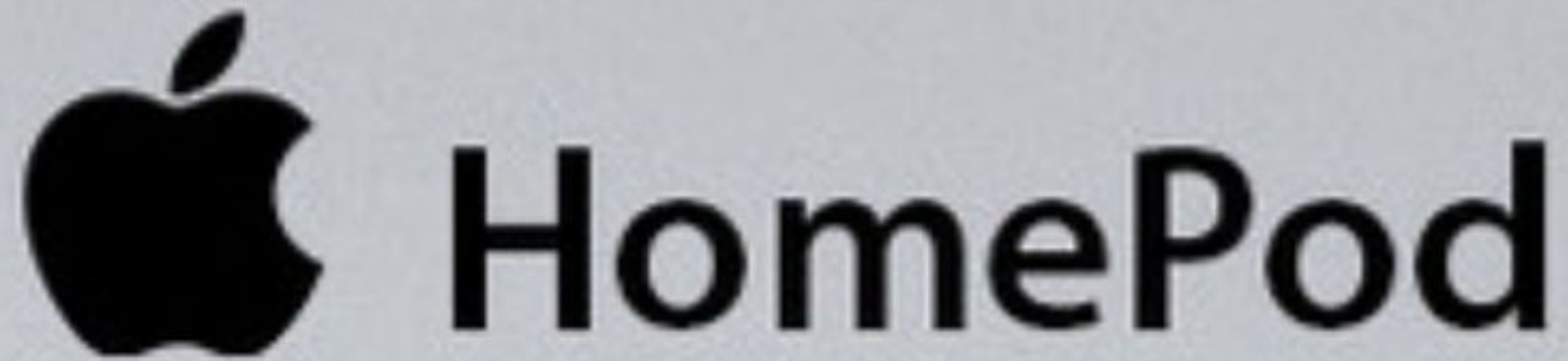


THREATS TO PRIVACY PERSONAL DIGITAL ASSISTANTS

These digital assistants are built on the latest technologies of speech recognition, predictive analytics, evolution of Big data, and faster processing speeds

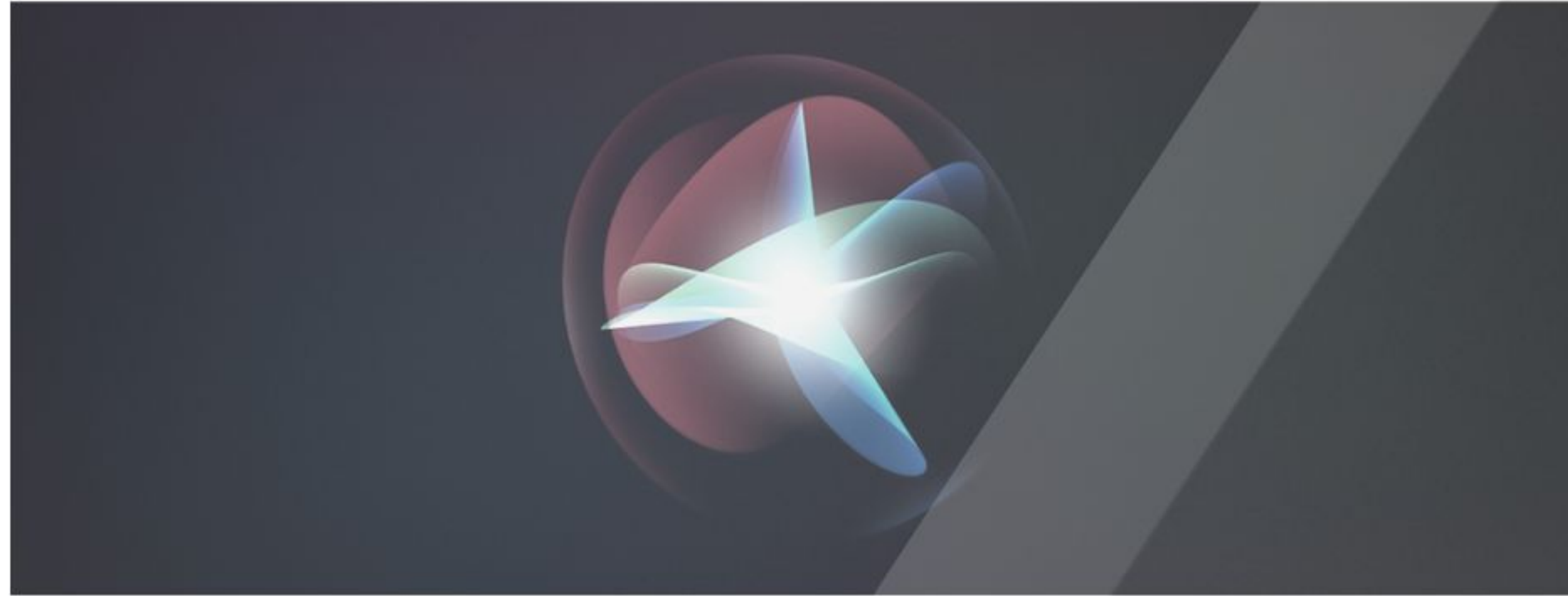
These are Siri, Google Home, Microsoft's Cortana, etc : They anticipate what users want and when they want it

But how much do humans want these digital assistants to know?

The logo for Apple HomePod, featuring the black silhouette of an Apple with a bite taken out of it, followed by the word "HomePod" in a bold, black, sans-serif font.

Apple introduced the iPhone 6 in 2014 which offered encryption functionalities such that user's data stored on the phone are automatically encrypted and can only be decrypted with the passcode that only the user possess. Even apple do not possess the passcode

Apple refused NSA's request for a backdoor into a terrorist phone, on privacy grounds, that to be globally competitive they must be able to assure consumers that their data is secure.



SECURITY APPLE'S SIRI

Apple's Siri aims to collect data on what apps you use, where you are, who you talk to or message, etc using these information about you, Siri can calendar your meetings and events, remind you to call people on their birthday's or start playing your favourite song when you are exercising in the morning, without asking: But it aims to do most of these processing on your phone, locally and when it needs to connect to its Servers (e.g to warn you of traffic ahead,) it assigns you a random number so Apple servers do not need to know your identity



Safeguards to Privacy - Apple vs Google

Apple aims to make a distinction between what your phone knows and what the company knows

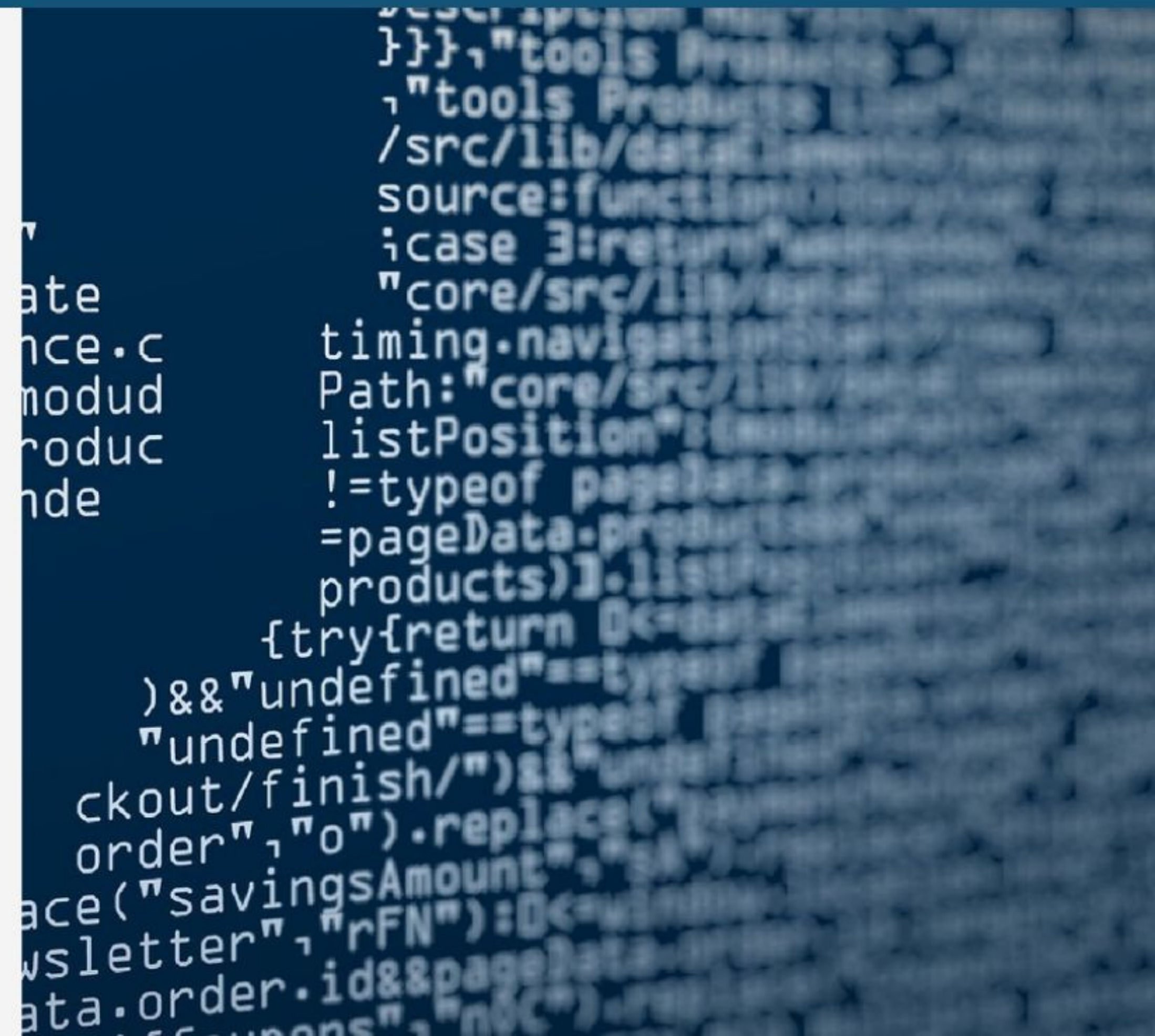
Google on the other hand appears to aggregate all your information from web searches, browsing history, use of gmail, Maps, google docs, calendar, Youtube as well as data from your (android) device-like location, app use, call&messaging data... on its servers which could be anywhere in the world

Google says it will not sell this information to advertisers, but will only use it to target ads to users

Data Security & Privacy

GOVERNANCE AND LEGAL

- **Information Rights:** What rights do individuals and groups have to their own personal data and to those of others?
- **Intellectual Property Rights:** How can IP rights be protected in a digital age?
- **Governance:** Should the Internet and e-commerce be governed by Public laws?



DATA PROTECTION PRINCIPLES

To be adequate, Data Protection & Privacy Legislation must follow Global norms governing Data Security and Privacy

1 USED FAIRLY AND
LAWFULLY

2 USED FOR LIMITED,
SPECIFICALLY STATED
PURPOSES

3 USED IN A RELEVANT WAY

4 ACCURATE

5 KEPT FOR NO LONGER
THAN IS ABSOLUTELY
NECESSARY

6 NOT TRANSFERRED
OUTSIDE OF THE COUNTRY
WITHOUT ADEQUATE
PROTECTION

7 HANDLED ACCORDING TO
PEOPLE'S DATA
PROTECTION RIGHTS

8 KEPT SAFE AND SECURE

The General Data Protection Regulation

The Four Pillars of the GDPR

PROOF OF CONSENT

Explicit consent by all Data Subjects is required
Data Recipients must use unticked opt-in boxes
Double opt-in is a good way to be compliant

RIGHT TO DATA PORTABILITY

Data Subjects have right to their data
Data Controllers must be able to provide users with their information
Data subject must be notified of any breach of subject's data within 72 hours

RIGHT TO ERASURE

Data subjects have right to be forgotten
Data Processor must be able to delete user entirely from its records
Data Controller must work with all processors to ensure user data is completely erased

RIGHT TO REFUSE PROFILE

Data subject can request not to be profiled based on personal information
Data subject cannot receive marketing campaign based on segmented Data

THE RIGHT TO BE FORGOTTEN

The Right to be forgotten — **Gonzalez vs. Google** Court of Justice of European Union

The Right of Individuals to request that certain links to personal information found through search engine be removed

The right to edit and delete personal information from the web

Unlike the EU, Whether individuals lose control over all personal information is still up for debate in the United States



DATA PROTECTION LAWS NIGERIA

For a very long time Nigeria lacked a single legal framework on data protection, what existed were bits and pieces of data protection provisions that were sector specific; together with other legal frameworks such as Section 37 of the 1999 Constitution, Freedom of Information Act, Cybercrimes Act, NCC Consumer Code of Practice Regulations, 2007, CBN Consumer Protection Framework, Credit Reporting Act, 2017 etc. The absence of a standardized data protection regime meant that citizen data was left unprotected and prone to manipulation.

On January 25, 2019, **The National Information Technology Development Agency (NITDA)** presented the **NITDA Data Protection Regulation 2019**, a welcome development to the data protection regime in Nigeria. The earlier NITDA Data Protection Guideline was the most ambitious effort at data protection in Nigeria.

The 2019 NITDA Regulation aims at safeguarding the rights of natural persons to data privacy; foster safe conduct of transactions involving the exchange of personal data; prevent manipulation of personal data and ensure that Nigerian businesses remain competitive in international trade; through the safeguards afforded by a just and equitable legal regulatory framework on data protection and which regulatory framework is in tune with global best practices.



DATA PROTECTION BILL 2015

More holistically, there is an ongoing effort by the National Assembly to pass a Data Protection and Privacy Law. The Data Protection Bill 2015 is currently before the House of Representatives. The Senate also has before it two Data Protection Bills. Both bills have been referred to the Senate expert group on ICT and Cyber Security to dissect and compile for a more comprehensive law- to the standard of the European GDPR



INDUSTRY SELF-REGULATION

Government Regulation alone is insufficient to protect Privacy. The technologies evolve quickly and Regulators will always play catch-up. The Online Industry in the US in particular has always argued that Industry can do a better job of protecting Privacy than governments

A conceptual basis of American Privacy law is notification and consent. Hence Terms of Use and Privacy Policies.

Privacy Policies of the likes of Facebook are shaping standards on the Internet. Developments in recent times have exposed gaps in Industry Self-Regulation hence the drive towards Co-Regulation



What are the implications for the
Financial services sector



REFERENCES

Harvard Journal of Law & Technology: Volume 30, Number 1, Fall 2016
“Get To Know Me: Protecting Privacy and Autonomy under Big Data’s Penetrating Gaze”

E-commerce : Business.Technology.Society
2018, Global edition, 14/ Kenneth Laudon, Carol Guercio Traver

Routledge Handbook of Media Law

Demands Grow for Facebook to Explain Its Privacy Policies
by Tiffany Hsu, nytimes.com

<https://www.lawyard.ng/wp-content/uploads/2019/01/Nigeria-Data-Protection-Regulation.pdf>



THANK YOU FOR
LISTENING

Rotimi Ogunyemi is an ICT Attorney -
Managing Partner of BAYO OGUNYEMI&CO a
member of JOHNSON&WILNER Technology
Lawyers

OGUNYEMISOLICITORS.ORG