

NATIONAL DATA WORKSHOP



Uche. M, Mbanaso Ph.D.

Executive Director, Centre for Cyberspace Studies,
Nasarawa State University, Keffi, Nigeria

Visiting Scholar: LINK Centre, University of the Witwatersrand,
Johannesburg, South Africa

Email: uche.magnus@mbanaso.org

Theme: Data Privacy and Security

Topic: Personal Data Privacy and Security – Who, What, When, Why, Where and How?





War Is Founded On Deception



Sun Tzu



Data Wars!



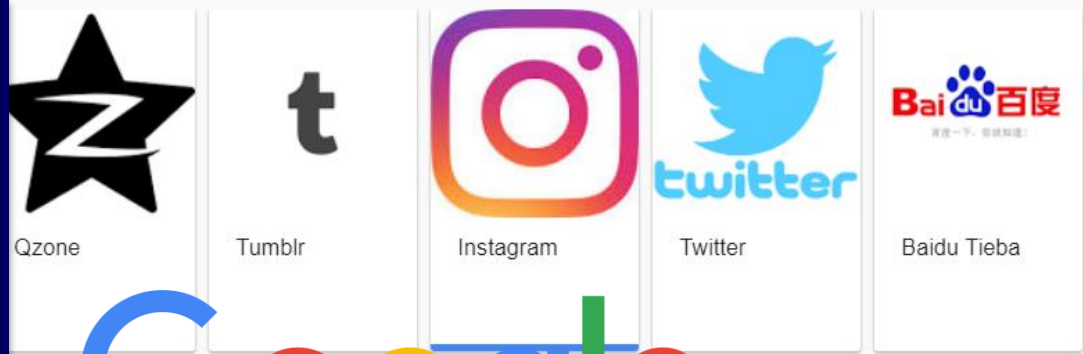
Deceive the data subject, keep him ignorant of your true data activities, and you shall profit more from data trading?

- Introduction
- The Six Privacy Data Axioms
- The EU General Data Protection Regulation (GDPR)
- Privacy Protection Architecture
- Discussions
- Conclusion

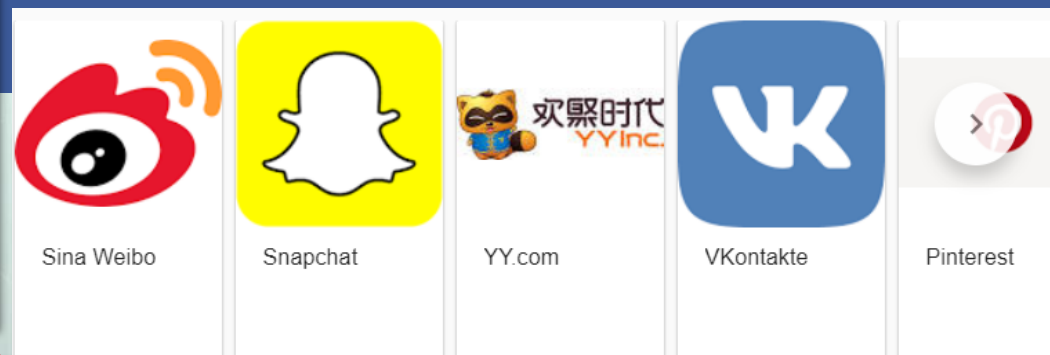
All Social Networks and Media trade on Data.

Personal data has become a priced commodity since many organisations harvest personal data for profit.

Personal data raises conflict and controversy.



Google
facebook




Top World Brands

X.1	2006	2017
1	Microsoft	Google
2	General Electric	Apple
3	The Coca-Cola Co.	Microsoft
4	China Mobile Games and Entertainment Group	Amazon
5	Marlboro	Facebook


<https://www.emarketer.com/Chart/Top-10-Brands-Worldwide-Ranked-by-Brand-Value-2006-2017-billions/209438>

Five of the top 10 brands in 2016, were retailers. While in 2017, nine of the top 10 brands in the world were User-Data Companies(UDCs).

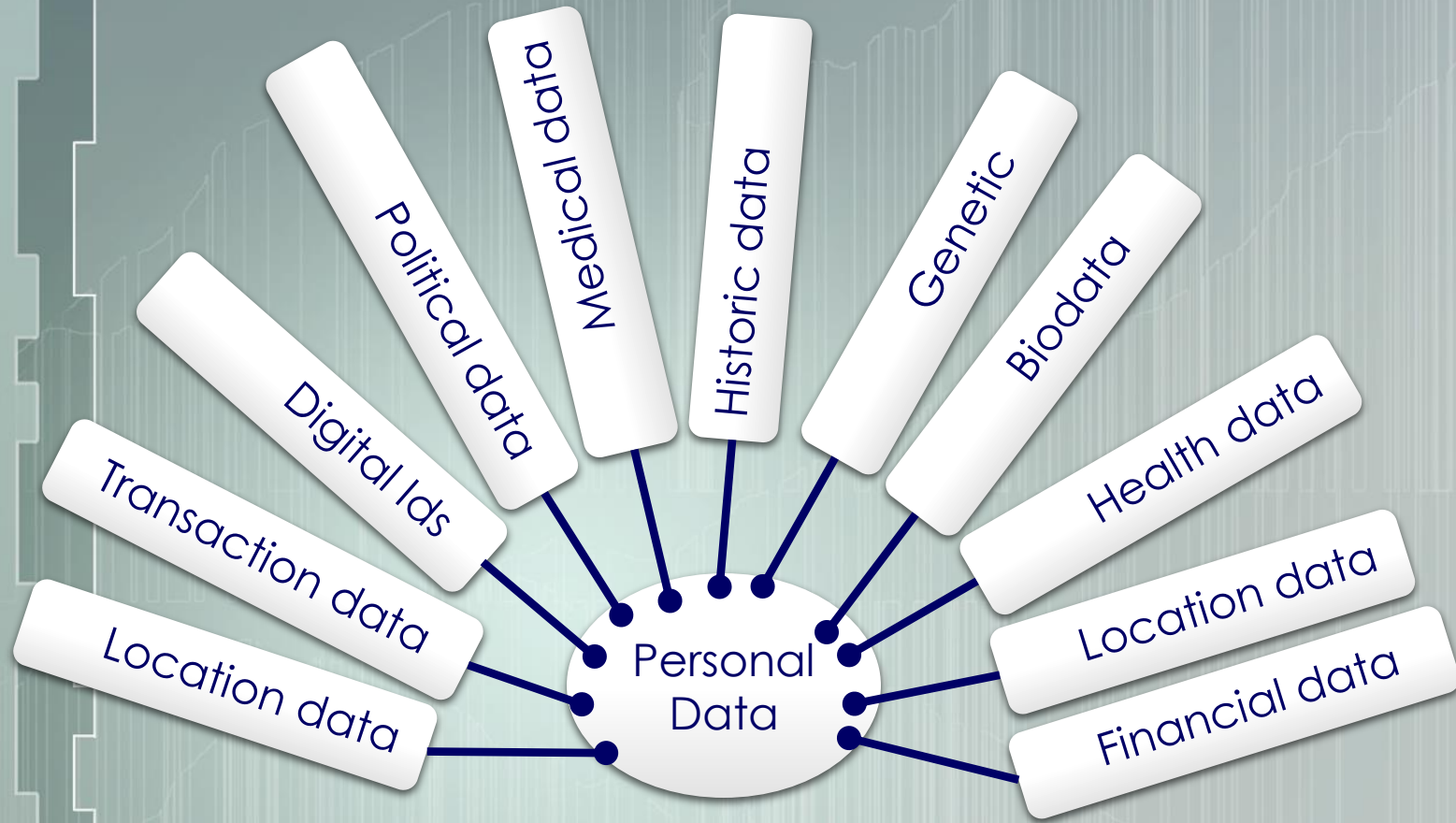
- Data has emerged the currency of the digital space, a priced commodity that has fuelled exceptionally amassing of information globally.
- It is now popularly acknowledged that personal data is used for marketing, shaping or forming opinions, and can influence political participation without recourse to the data owner.
- These massive violation of privacy has generated serious concerns across the globe as current privacy protections fall short of protecting users from data misuse, abuse or breaches.



Personally Identifiable Information (PII) data



- PII has become the attraction of most of data breaches, and it is any information that could possibly identify or trace (or link) a particular individual.
- Any information that can be used to extricate one person from another and can be used to associate (de-anonymizing) anonymous data.



• The data that concerns us, links us, associates us, reveals us, and can potentially lead to our harm is huge and fluid.



Introduction

The Six Privacy Data Axioms

The EU General Data Protection Regulation (GDPR)

Privacy Protection Architecture

Discussions

Conclusion

Outline

The Six Privacy Data Axioms



Sharing data can offer some benefits, but **what** you share, and **who** you share, **why** you share, **when** you share, **where** you share and **how** you share should be entirely individuals right to privacy!



- **What** identifies categories of PII that can be collected irrespective of unsettled use of them?
- **Who** identifies the entities or mechanisms that collect PII regardless of the purpose and lawfulness?
- **Why** refers to the purpose of collection or reason adduced from the collection or processing?
- **When** describes the instance of use i.e. the situation under which the data is collected, processed or shared.
- **Where** depicts the platform or mechanism used in the collection, sharing or processing?
- **How** refers to the channel or means of collection, processing or sharing?



What

- **Biodata**
- **Biometrics**
- **Genetic**
- **Locations**
- **Digital Behaviour**
- **Digital Transactions**
- **Digital Ids**
- **Historical data**
- **Medical data**
- **Financial data**
- **Professional/career data**
- **Fitness activity**
- **Music/Movies**
- **Political views**
- **others**





Who

- *AI*
- *Smart Devices (IoT)*
- *Social network/media*
- *Corporate organisations*
- *Nation States*
- *Organised criminal gangs*
- *Terrorists*
- *Hacktivist*
- *Search engines*
- *Others*





Why

- ***Marketing***
- ***Advertisement***
- ***National Security***
- ***Crime***
- ***Fraud***
- ***Politics***
- ***Recruitment***
- ***Services***
- ***Promiscuous permission***
- ***Access control***
- ***Others***





When

- ***App installation***
- ***Online shopping***
- ***Social interactions***
- ***Online application forms***
- ***Online banking***
- ***Account creations***
- ***Surfing/Searching***
- ***Gaming/gambling***
- ***Others***





Where

- ***Social networks and media sites***
- ***E-commerce sites***
- ***Government sites***
- ***Apps usage***
- ***Smart Personal Devices***
- ***Access control process***
- ***Home devices***
- ***Others***






How

- ***Online Forms***
- ***Promiscuous permissions***
- ***Enrolments***
- ***Content access***
- ***Tracking/surveillance***
- ***Cookies***
- ***Sign In/ Sign Out***
- ***Others***



- Introduction
- The Six Privacy Data Axioms
- The EU General Data Protection Regulation (GDPR)
- Privacy Protection Architecture
- Discussions
- Conclusion

General Data Protection Regulation (GDPR)



GDPR is an EU legal framework that describes set of rules that regulates the collection and processing of citizens personal data within the EU territory, and beyond.

General Data Protection Regulation (GDPR)

- GDPR is privacy centric with well crafted rules, roles and responsibilities.
- It creates the backdrop to ***identify, protect, detect, respond*** and ***recover***¹ in relation to data breaches.

1. NIST Cybersecurity Framework

GDPR Core Pillars



Principles

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability principle
- Lawful basis for processing
- Consent
- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests
- Special category data
- Criminal offence data



Individual rights

- Right to be informed
- Right to be forgotten
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related to automated decision making including profiling



Accountability and Governance

- Contracts
- Documentation
- Data protection by design and default
- Data protection impact assessments
- Data protection officers
- Codes of conduct
- Certification

- GDPR defined the type of data for which notification is required after a breach, and who should to be notified, how the notification has to be carried out, and whether specific authorities have to be notified – processes are cumbersome!
- Typically breaches involving personal, financial and health data are subject to notification requirements but exact definitions vary in different jurisdictions.
- Organisations doing business globally may have customers in many jurisdictions and may have to comply with a variety of requirements. The costs of such a process together with legal penalties, possible compensation for damages and any resulting lawsuits can be high enough to constitute an existential threat to some organisations.

- The consequences to businesses that may experience data breaches can be onerous.
- Generally, regulatory obligations place heavy burden of proof on businesses concerning personal data processes.
- How to validate and prove that individual rights are enforceable within the span of organisational context.
- Burden of proof to demonstrate that processor's legitimate grounds override the interests of the data subjects.
- Where multiple parties share data, who bears burden of proof concerning processing activities.
- Technically, how do data subjects exercise their rights to privacy?



Outline

- Introduction
- The Six Privacy Data Axioms
- The EU General Data Protection Regulation (GDPR)
- Privacy Protection Architecture
- Discussions
- Conclusion

Data Privacy Protection Challenges

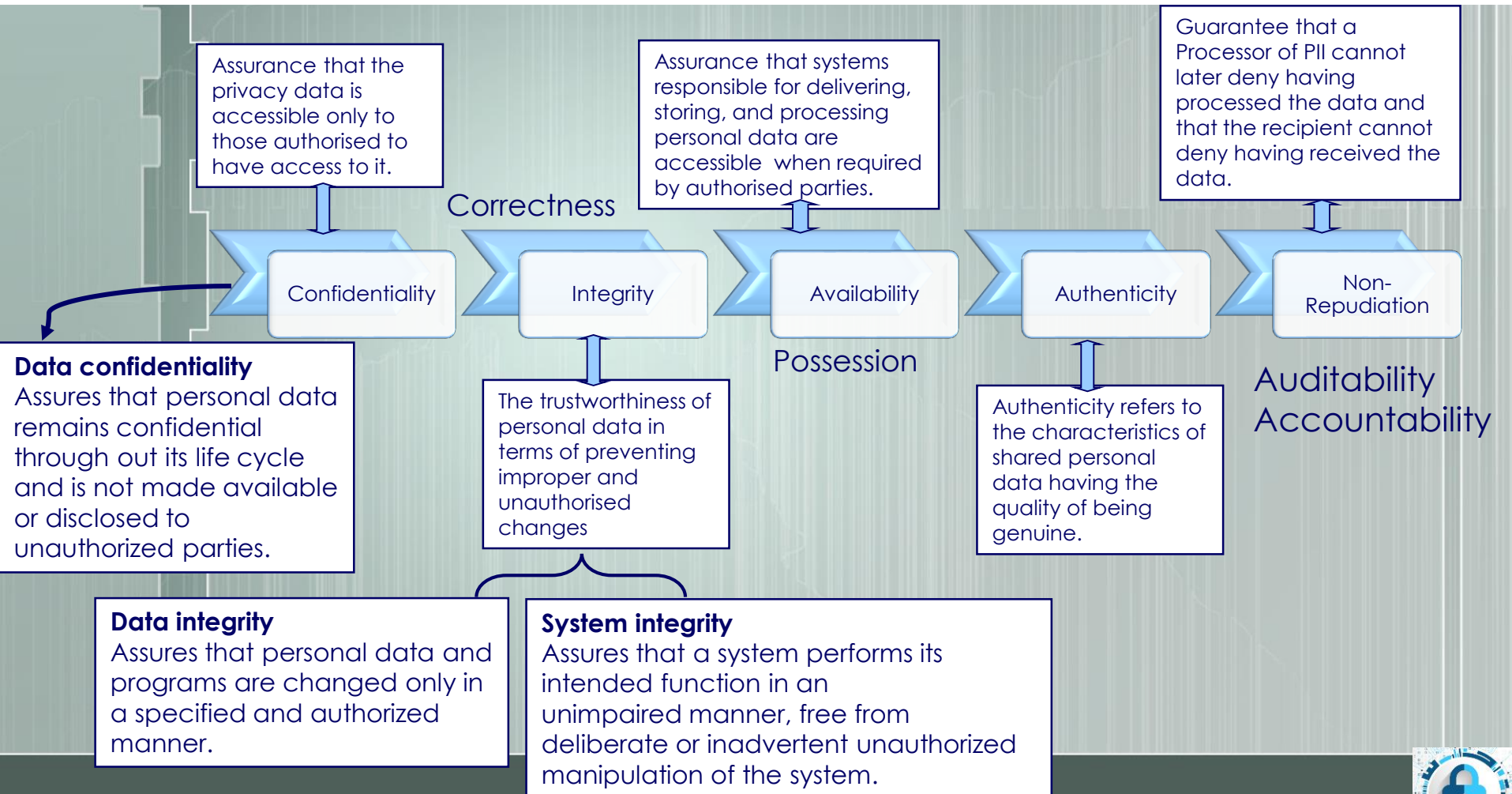
- Privacy Data is fluid across the global digital space;
- Average data subject is unaware of the consequences, safeguards and rights in respect to PII;
- Data subject's inability to classify sensitivity of personal data;
- Data subject usually grants permissions to greedy data gladiators without the ability to balance the benefits of the services rendered and associated risks;
- Data subject in many instances have no option than to tick the privacy statements without understanding the terms and associated risks;
- Data subject's inability to monitor and track personal data in the global digital space is a huge task and burdensome;
- The complexity in interconnected or integrated systems, especially, in application to application data transactions;
- Technology to automate all aspects of privacy rights is still work in progress.

Goals of Data Security and Privacy Protection

Utility: The value of privacy data comes from the characteristics it possesses

Privacy

Assures that the individual controls or influences the collection and processing of personally identifiable information (PII).



Privacy Protection Architecture Construct

Requirements

Party A's requirements,
that party B must fulfil.

Capabilities

Party A's capabilities,
that is willing and able
to give to party B, if
conditions in
Requirements are met
by B.

Party A Policy

Requirements

Party B's requirements,
that party A must fulfil.

Capabilities

Party B's capabilities,
that is willing and able
to give to party B, if
conditions in
Requirements are met
by A

Party B Policy

Privacy Protection Architecture

- **Requirements** can be used to express a party's obligations (or commitments), it would expect privacy data requesting party to fulfil before it can release such data;
- **Capabilities** can be used to express the competences (or services or features) of the relying party that it is willing to release to the requesting party, once conditions expressed in the *Requirements* section are satisfied.
- Thus, *Requirements* and *Capabilities* form elements of policy framework that can be used between two or more cooperating privacy protection entities to guarantee confidentiality, privacy and trust dynamically and concurrently too.

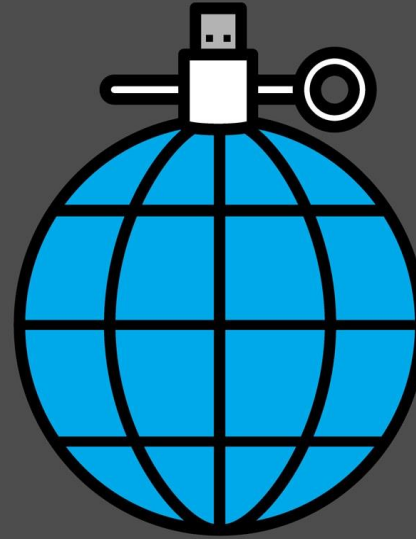


Outline

- Introduction
- The Six Privacy Data Axioms
- The EU General Data Protection Regulation (GDPR)
- Privacy Protection Architecture
- Discussions
- Conclusion

The Next Cold War Is Here, and It's All About Data

Source: <https://www.wired.com/story/opinion-new-data-cold-war/>



Discussions

Discussion

- **Data has been promoted as fuel of success in the digital society, and the highest priced data commodity is PII.**
- **PII is used in a variety of forms and shapes, including profiling, marketing, advertisement, political opinion, digital fraud, etc.**
- **Consequently, safeguarding personally identifiable information within and across borders, is increasingly important for both offline and online activities but difficult to achieve.**
- **But there is a momentous struggle for data dominance**

Discussion

- Facebook allowed Cambridge Analytica (CA) to continuously amass data resulting to over 50 million of Facebook users' data allegedly compromised.
- By GDPR imposed restrictions on the transfer of PII across borders, CA data breach carries serious consequences.
- But how did CA harvest those data from Facebook?
- Technically, through Facebook API integration or Web Services call!
- API or Web Services are granted access by the use of cryptographic token - a promiscuous permission.
- Most API or Web Services exposed services, lack granular access control restrictions!

Discussion cont'd

- With promiscuous permission CA had unrestricted access to Facebook data!
- Thus, sharing PII by parties using API or Web Services exposes PII to huge risks!
- Monitoring and tracking *what is collected by who, when, where and how*, technically is not a trivial task?
- Again, sharing of PII can be cascaded as there is no limitation by GDPR, i.e. third party A to B, and from party B to part C!
- API or Web Services are granted access by the use of cryptographic token - a 'promiscuous permission'.
- These Use Cases raise fresh research questions on the preservation of individual privacy!

Discussion cont'd

- More so, addressing and automating GDPR's 9 privacy rights based on 16 principles, technically, requires a robust Privacy Protection Architecture with efficient protocols!
- Thus, the proposed Privacy Protection Architecture by Policy Construct of *Requirements* and *Capabilities* with appropriate evaluation engines can be the basis to address some of the privacy challenges!

Hey! Shouldn't a Data Subject benefit from the proceedings of personal data trade?





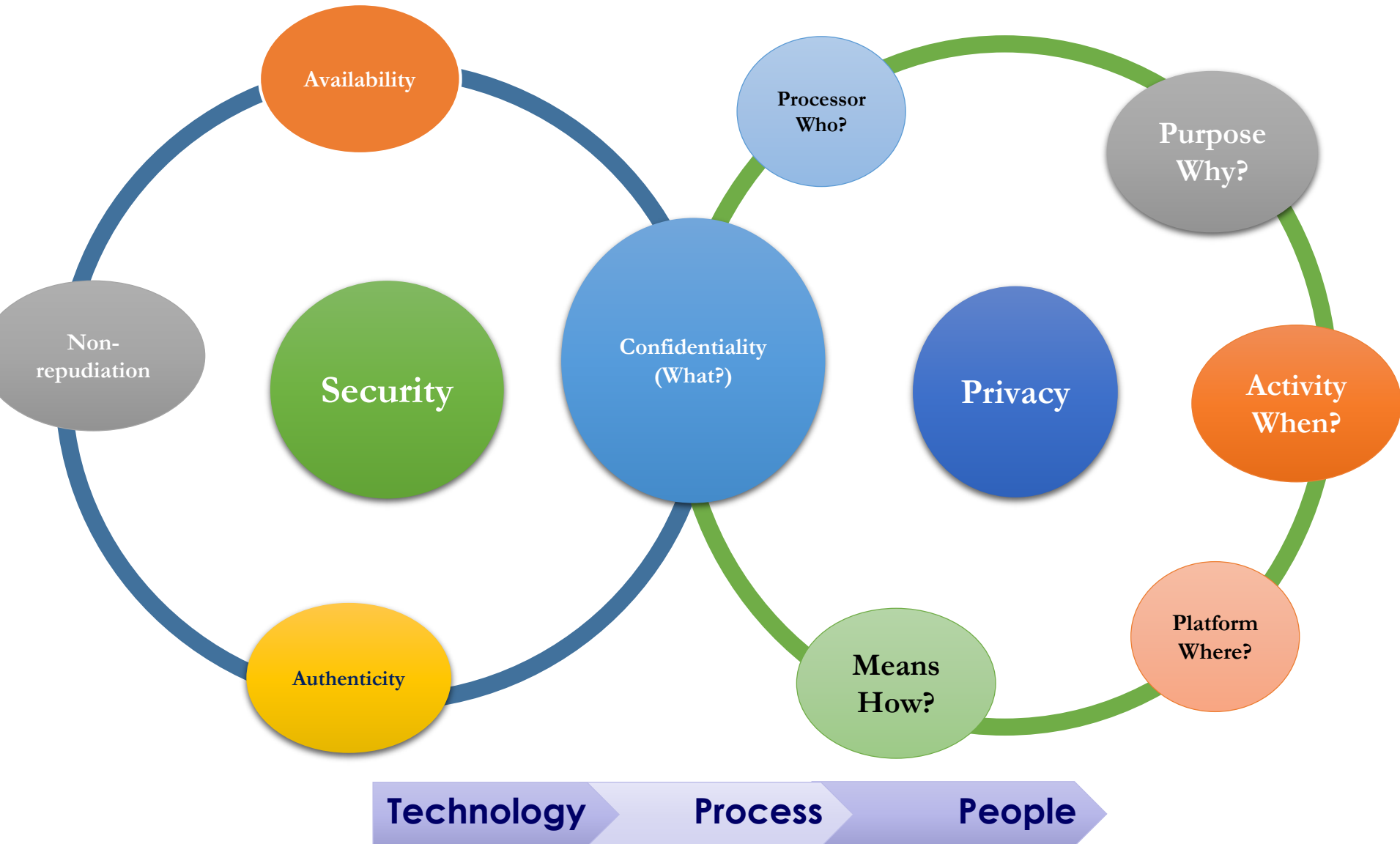
Call for Action



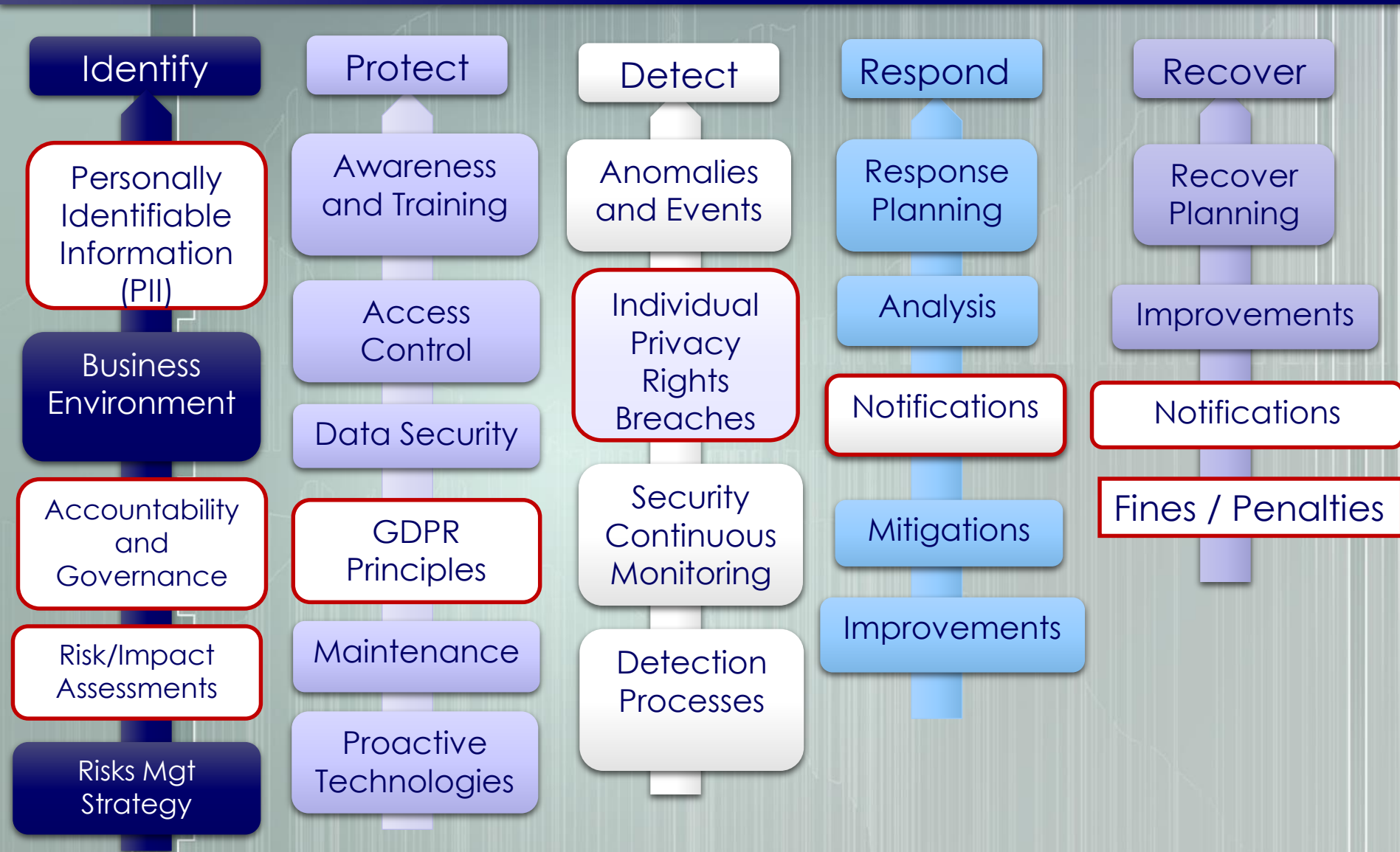
Data Privacy Protection Postulations

- How can a data subject really track and monitor which personal data is accessed and by who?
- How can a data subject really be notified in real-time when privacy data is shared with third parties who?
- What are the protocols to hold a third party accountable in relation to compromised privacy data?
- How can a party guarantee that the privacy rights of a data subject based on GDPR can be respected by (international) remote third party?
- How can a party assure data subject that a third party privacy protection mechanism supports GDPR's accountability and governance technically?
- How can disputes and liabilities be handled technically? Is there a respected channel for handling and resolving disputes?
- Whose fault is it in the event of a problem with mutually shared privacy data?
- Is there any hard-to-repudiate digital evidence that parties can use in courts of law to support their claims?

Data Security and Privacy Intersection



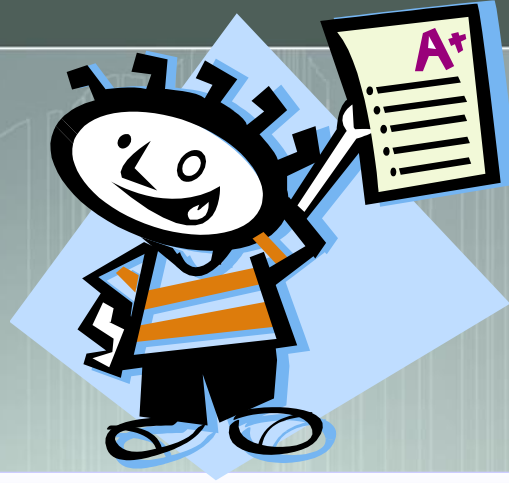
NIST Cybersecurity Framework > Data Security and Privacy



- Introduction
- The Six Privacy Data Axioms
- The EU General Data Protection Regulation (GDPR)
- Privacy Protection Architecture
- Discussions
- Conclusion

Conclusion

- Technical capacity to protect PII dynamically and in real-time still requires more research inputs from the research community;
- The six privacy data axioms and the privacy protection postulations presented here can obviously stimulate more research inquiries;
- Interpretation and implementation of GDPR is still subject to a variety of differences – philosophically, privacy is highly influenced by many factors;
- Some privacy factors are dynamic, and some are static;
- Privacy protection hinges on effective technology, policy and law;
- Automation of privacy rights, and intelligent privacy protection architectures can help enforce GDPR better.



If we cannot find a solution, then it is not a problem

We will either find a path or we create one

Uche. M, Mbanaso

Ph.D. Information and Communications Security
Executive Director, Centre for Cyberspace Studies,
Nasarawa State University, Keffi, Nigeria

Visiting Scholar: LINK Centre, University of the Witwatersrand, Johannesburg, South
Africa

Email: uche.magnus@mbanaso.org