



NATIONAL JUDICIAL INSTITUTE

**THE JUDICIARY
IN THE EMERGING GLOBAL
AND DIGITAL SPACE**

15TH - 17TH AUGUST, 2022



DATA PRIVACY: STORAGE, RETRIEVAL AND PROTECTION

Presentation by

Asaolu Funmi

Chief Database Administrator

IT Unit, BPRS Department,

National Judicial Council

3 Outline

1. Data Privacy Terms
2. Data Privacy Concept
3. Importance of Data Privacy
4. Components of Data Privacy
5. Elements of Data Privacy
6. Data Privacy Legislation
7. Data Privacy And Data Protection Law In Nigeria
8. Data Governance
9. Data Privacy Best Practises
10. Role of Data Privacy in Government
11. Data Storage
12. Data Storage Devices
13. Data Retrieval
14. Advantages of Data Retrieval
15. Retrieval Data Samples
16. Retrieval Protection
17. Recommendations
18. References

4 DATA PRIVACY TERMS

- **Data** is any set of characters that is gathered and translated for some purpose or information that has been formatted into a form that is efficient for processing or facts and statistics collected for reference or analysis. Data can exist in a variety of forms — as numbers or text on pieces of paper, as bits and bytes stored in electronic memory, or as facts stored in a person's mind.
- **Types of data** are character, Boolean (true or false), Text (string), Number (integer or floating-point), Picture, Sound, Video
- Data Subject refers to any individual person whose personal data is collected, held or processed, who can be identified, directly or indirectly via an identifier such as a name, an ID number, height, an address
- A Data Owner make decisions such as who has the right to access and edit data and how data should be used hence responsible for Data Governance outcomes
- A Data Steward is responsible for the Data Governance tasks required to achieve those outcomes.
- Data custodians are responsible for the safe custody, transport, storage of the data and implementation of business rules



5 DATA PRIVACY CONCEPT

- **Data Privacy** involves setting access controls to protect information from unauthorized parties, getting consent from data subject where necessary, free from intrusions by the state, and maintaining data integrity. It is data management that deals with handling data in compliance with data protection laws, regulations, and general best practices.
- **Data privacy** is the proper handling of sensitive data such as personal data, confidential data like financial data and intellectual property data to meet regulatory requirements, the confidentiality and immutability of the data.
- **Data Privacy** focuses on information about individuals. Privacy rules determine what types of Personally Identifiable Information (PII) may be collected, about whom, to what extent, and what can be done with it. Businesses must ensure that only the appropriate access rights are granted to people in the organization, to partners with which they share data, and to the general public.
- **Personal Data** otherwise referred to as PII means any information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.)
- **Data Sovereignty** as part of data privacy laws especially for **Cloud Service Providers** is the concept that data is subject to the laws of the location in which it is collected, and data must be hosted on servers within the geographical region where the data is collected



6 IMPORTANCE OF DATA PRIVACY

Why is Data Privacy important?

- 1. Business Asset Management:** Data is perhaps the most important asset a business owns. We live in a data economy where companies find enormous value in collecting, sharing and using data about customers or users, especially from social media. Transparency in how businesses request consent to keep personal data, prevention of fraudulent activities, hacking, phishing, and identity theft, abiding by the privacy policies, and to manage the collected data, is vital to building trust with customers who naturally expect privacy as a human right.
- 2. Regulatory Compliance:** Managing data to ensure regulatory compliance is very important. A business may have to meet legal responsibilities about how they collect, store, and process personal data, and non-compliance could lead to a huge fine. If a business becomes a victim to a hack or ransomware, the consequences in terms of lost revenue and lost customer trust could be devastating.



7 COMPONENTS OF DATA PRIVACY

- Data Lifecycle
- Data Ethics
- Data Quality
- Access Control
- Data Integrity
- Data Security

8 COMPONENTS OF DATA PRIVACY (contd.)

- **Data lifecycle:** Different stages that a particular unit of data passes through from its initial generation or collection till it is archived or deleted at the end of its useful life. The data lifecycle for PII must begin with a clear purpose for collecting user data.
- **Data ethics:** Ethics extend beyond lawfulness and compliance with data privacy regulations. Ethical behaviour towards personal data includes transparency, openness, and fairness regarding how that data is handled.
- **Data quality:** While ensuring the accuracy of critical business data, data privacy professionals should maintain data consistency throughout an organization and fix data errors and inconsistencies. For example, if parties records are not up to date, wrong judgement might be passed.
- **Data Privacy** is related to, but not the same as, data security. They do have some overlapping obligations or functions as listed below:
 - **Access control:** Preventing unauthorized access to and use of data is the cornerstone of privacy, and possible only through security.
 - **Integrity of the data:** Making sure that data is accurate and not altered is both a privacy and a security concern.
 - **Accountability:** It is taking responsibility for what you do with personal data and compliance with company documented policies as regards to privacy and security.
- **Data Security** ensures the confidentiality, integrity, and availability of all data. Security professionals implement cybersecurity measures like authorization and data encryption to prevent data breaches, vulnerabilities and defend against malicious attacks.

9 ELEMENTS OF DATA PRIVACY

- Legislation
- Policies and Rules
- Best Practise
- Data Governance
- Global Variation
- Third Party Contact

10 DATA PRIVACY LEGISLATION

- **Data Privacy Legislation** is being enacted all the time, many countries have passed data laws and acts hence the regulations to comply with depend on where your organisation operates, what borders you do business across, and the regulation of the industry you are involved.
- The legal landscape is always shifting, and data legislation is still evolving. It is important to be acquainted with laws and regulations that affect your business operations hence completing due diligence is very important
- The most prevalent regulations (GDPR, CCPA, HIPAA, NDPR etc)
- **The Nigerian Data Protection Regulation, 2019 (NDPR)**
- GDPR: General Data Protection Regulation
- California Consumer Privacy Act (CCPA)
- Health Information Portability and Accountability Act (HIPAA)
- EUGDPR: The European Union's General Data Protection Regulation
- The right to privacy was included in the United Nations' Universal Declaration of Human Rights way back in 1948.
- Other data legislation that may affect your business could include cybercrime laws, online transaction laws, and consumer protection law. The Children's Online Privacy Protection Act (COPPA) ensures information privacy for minors in the US.

DATA PRIVACY AND DATA PROTECTION LAW IN NIGERIA

- NITDA Regulation - The NITDA Act empowers the National Information and Technology Agency (NITDA) to issue guidelines to cater for electronic governance and monitoring the use of electronic data exchange. Deriving from this provision, NITDA then developed and issued the Nigeria Data Protection Regulation 2019.
- Cybercrimes (Prohibition, Prevention etc) Act 2015 (CPPA)
- Central Bank of Nigeria Consumer Protection Framework 2016 (CPF)
- The Nigeria Communications Commission (Registration of Telephone Subscribers) Regulations 2011 (NCC Regulations)
- The Credit Reporting Act 2017 (CRpA)
- The Nigeria Data Protection Regulation 2019

12 DATA GOVERNANCE

- Data Governance is the principle of managing data availability, usability, integrity and security during its life cycle, from acquisition to use to disposal, based on internal data standards and policies that also control data usage.
- A data governance is the collection of rules, processes, and role delegations; the framework that facilitate data sharing and preserves data privacy and dictates how the data is collected, shared and used.
- Data governance is closely associated with data quality improvement efforts; metrics that document improvements in the quality of an organization's data are central to demonstrating the business value of governance programs.
- Data quality techniques include data profiling, in terms of accuracy, completeness, consistency, reliability and whether it is up to date. It checks data sets to identify errors, data cleansing, also known as data scrubbing, which fixes data errors by modifying or deleting bad data; and data validation, which checks data against pre-set quality rules.



13 DATA PRIVACY BEST PRACTICES

- **1. STORE PAPER FORMS SECURELY:** Much like electronic data, paper documents such as consent forms, printouts, or case tracking sheets that contain personal identifying information (PII) must be stored securely in locked file cabinets when not in use and must be handled only by trained staff members when actively used during research. With consent forms in, it is important to remember that physical separation of the form from the subject's data is not sufficient.
- **2. USE SECURE STORAGE FOR DETACHABLE MEDIA:** Confidential data stored on transportable media such as CDs, DVDs, flash memory devices, or portable external drives must be stored securely in a safe or locked file cabinet and handled only by authorized staff members.
- **3. PROTECT PASSWORDS:** Secure data storage depends on the creation and use of passwords that are needed to gain access to data records. The best storage and encryption technologies can be easily undone by poor password practices. Passwords should be difficult to determine and be protected as carefully as confidential data. They should never be shared or left on slips of paper at workstations or desks. Password must be changed periodically.



14 DATA PRIVACY BEST PRACTICES (contd.)

- **TRAIN AND MONITOR RESEARCH ASSISTANTS:** Research assistants and staff who work with confidential data should understand and follow all of the basic data security practices governing their work schedule according to various training and orientation programmes. Research assistants and other staff must be acquainted with procedures and practices in the prescribed industry guidelines.
- **RESTRICTED USE SHARED ACCOUNTS OR GROUP LOGIN IDs:** Anyone who works with confidential electronic data should identify themselves when they log on to the PC or laptop computer that gives them access to the data. Use of group login IDs violates this principle. It is important that everyone working with confidential data has a unique password that personally identifies them before they can access the data.
- **KEEP USER GROUP LISTS UP-TO-DATE:** User groups are a convenient way to grant access to shared folder or files stored on a remote server. Creation of user groups simplifies the granting and revoking of access. By granting access privileges to each of the folders to the group as a whole, newly authorized members of the team can obtain access to all related electronic data resources by being added to the group. When an individual is no longer a part of the team, the removal of his or her ID revokes access to all resources. Group membership lists should be reviewed regularly and, when a staff complete their work or leave a team, the user group administrator should update the user group list so that the person cannot have access any shared resources.
- **AVOID USING INDIVIDUAL PCs OR LAPTOPS FOR COLLECTION OR STORAGE OF CONFIDENTIAL DATA:** The organisation oversees the use and maintenance of computers for collection and storage of confidential or personal data. The institutionally owned computers and managed computing platforms should be engaged for confidential or personal data because individual computers may lack adequate firewalls, virus protection, and encryption required for protection of confidential data. The institutionally owned computers should have up-to-date maintenance that are designed to keep PCs, laptops and their contents securely protected from theft or unauthorized use.

15 DATA PRIVACY BEST PRACTICES (contd.)

- **ACTIVATE LOCK OUT FUNCTIONS FOR SCREEN SAVERS:** Computers used for data analysis should be configured to "lock out" after 20 minutes of inactivity to reduce the risk of theft or unauthorized use of data in situations where a user working with confidential data leaves his or her desk and forgets to logoff the PC.
- **USE SECURE METHODS OF FILE TRANSFER:** Transfer of confidential data files between users or between institutions has the potential to result in unintended disclosure. File transfers are often the weakest part of any plan for keeping data secure. Folders and files with PII or other confidential information should always be compressed and encrypted before they are transferred from one location to another especially when transferring files as attachments to email or as files on physical media such as CDs or flash memory drives. File compression minimizes the chances of your file transfer failing because your file is too large. Encryption will ensure that your compressed file cannot be read by anyone who does not have the password that was created when the file was compressed and encrypted. Other secure and convenient methods of file transfer include SharePoint and institutionally-supported Google Drive cloud service provider
- **USE EFFECTIVE METHODS OF DATA DESTRUCTION:** There must be a plan for the ultimate disposal of obsolete data which specifies what will be done with the data once the data collection objectives are completed. In many cases, de-identified data file for use by others or the general public. If your plan calls for destruction of documents or electronic files after the task is completed, all paper files or CDs with PII should be shredded and any electronic files on memory drives, PCs, laptops and file serves should be permanently deleted. In general, regulation requires that all raw data be kept for a minimum of 5-years after task completion. If the task plan includes long term retention of PII (in paper or electronic form) then all data files should be stored securely in a safe or locked file cabinets in a secured building.

16 ROLE OF DATA PRIVACY IN GOVERNMENT ORGANIZATION - JUDICIARY

- ❖ **ADHERENCE TO COMPLIANCE REQUIREMENTS AND STANDARDS**
- ❖ **PREVENTION OF BREACHES THAT COULD LEAD TO NEGATIVE IMPACT ON THE JUDICIARY** - professionals, under no circumstance, should not allow themselves to be used to leak UNDELIVERED JUDGEMENT
- ❖ **ENHANCE INTEGRITY AND UPHOLD THE RULE OF LAW** - data (records) serve as the backbone in the administration of justice so accurate records provide complete information that influence fair and impartial decision making in the courts.
- ❖ **PREVENTION OF BREACHES THAT COULD DAMAGE THE IMAGE OF DATA SUBJECTS / INDIVIDUALS**

17 DATA STORAGE

- Storage refers to maintaining information over time; **DATA STORAGE** is a general term for archiving data in electromagnetic or other forms for use by a computer or device.
- Digital data storage is essentially the recording of digital information in an electronic storage medium.
- The storage device typically enables a user to store large amounts of data in a relatively small physical space and makes sharing that information with others easy. The device may be capable of holding the data either temporarily or permanently.
- Digital data storage devices have many uses, for example, computers usually rely upon information storage to function. Storage media can also be used to back up important information (storing digital data can involve durability and reliability issues, so making independent copies of information is a sensible precaution).
- Some storage devices are also portable, meaning that they can be used to transfer information from one computer or location to another.



18 DIGITAL DATA STORAGE DEVICES

1. USB Flash Drives
2. Floppy Disks
3. Compact Discs (CDs)
4. Tapes
5. DVD and Blu-ray Discs
6. Hard Drive Disks (HDDs are a legacy storage technology that use spinning disks to read/write data).
7. Secure Digital Cards (SD Card) - is a very small flash memory card. SD cards are used in smartphones, digital cameras, e-books and car navigation systems
8. Solid-State Drives (SSDs) are faster and more efficient than HDDs. HDDs are priced lower, but SSD are expensive though the price is dropping.

19 DIGITAL DATA STORAGE DEVICES (contd.)

9. Cloud Storage

Cloud storage is a cloud computing model that stores data on the internet through a cloud computing provider who manages and operates data storage as a service. It is delivered on demand with just-in-time capacity and costs, and eliminates buying and managing your own data storage infrastructure. Examples are iCloud Drive, Dropbox, Microsoft OneDrive, Google Drive etc

- Microsoft OneDrive is a file hosting service operated by Microsoft. First launched in August 2007, it enables registered users to share and synchronize their files. OneDrive also works as the storage backend of the web version of Microsoft Office.
- Dropbox offers one central hub for online file storage, file sharing, and syncing. Whether you are at work or on the road, your files are synced across your devices and accessible in real time.
- Google Drive is a file storage and synchronization service developed by Google launched on April 24, 2012. Google Drive allows users to store files in the cloud, synchronize files across devices and share files

10. Punch Cards - A punched card is a piece of stiff paper that holds digital data represented by the presence or absence of holes in predefined positions



20 DATA RETRIEVAL

- **Data Retrieval** - The process by which data is selected and extracted from a file, a group of files, or a database. Retrieval is the ability to access data or information when needed.
- **Data Retrieval** is the retrieval of items (objects, Web pages, documents, etc.) which satisfy specific conditions set in a regular expression like a query. Data retrieval is a term used to describe the process of searching for, locating, and returning data that aims at determining which documents contain the exact terms of the user queries. Data retrieval include fetching large amounts of data, usually in the form of reports, for example, a user may retrieve a document on a computer to be viewed or modified.
- **Data Retrieval** could mean obtaining data from a database management system such as ODBMS it is considered that data is represented in a structured way, and there is no ambiguity in the data. In order to retrieve the desired data the user present a set of criteria by a query. Then the Database Management System (DBMS), software for managing databases, selects the demanded data from the database. The retrieved data may be stored in a file, printed, or viewed on the screen. In databases, data retrieval is the process of identifying and extracting data from a database, based on a query provided by the user or application. It enables the fetching of data from a database in order to display it on a monitor and/or use within an application.



2 | **ADVANTAGES OF DATA RETRIEVAL**


- To retrieve the desired data the user present a set of criteria by a query which eliminate ambiguity in data.
- It saves the time of the user when they search for their necessary data or information
- The searching process is easy to understand
- It allows users across different parts of the system to use the same data and access multi-databases to use multiple keywords/concepts at the same time
- It makes available the current information in the storage database for consumption and further usage.
- It significantly increases a business owner's and consumers confidence in the data storage



RETRIEVED DATA SAMPLES

- Retrieval Data can be presented as Reports, forms, graphs, tables, pictures etc.

Investigation Report Sample

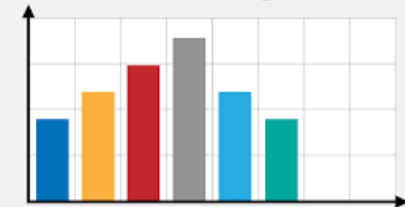
Inspection	100%
Investigation Report	100%
Background Information of the Subject	
Full Name	Bryan Milone
Contact Number	706-569-8708
Email Address	bmilone@fairwaynorton.io
Type of Case 100%	
Identify the type of case.	Complaint
Complaint Summary	
On February 20, an anonymous tip was received through the Fairway Norton Employee Hotline that accounts payable clerk, Bryan Milone, has allegedly been stealing company property. The source said that she saw Bryan packing 2 newly delivered optical mouse in his bag on February 18.	
Evidence	
Select and take/ attach photos of physical evidence.	Footage Security access records
CCTV footage shows Bryan holding a desktop monitor at 11:17PM on January 18, 2019. (Court order for release of CCTV records granted)	
 <p>Photo 1</p>	
Detail all conducted interviews by tapping ADD INTERVIEW.	
INTERVIEW 1	
Full Name	Shauna Sigmon
Conducted on	26.02.2019 14:41 PST
Interview Location	7th Flr., FNI Bldg., Roosevelt Ave., Farrar Parade, Western Australia

iAuditor
by VeriGator

The proportion of income adults and children spent on 4 common items in the UK in 1998

	food	electronic equipment	music	videos
adults	25%	5%	5%	1%
men	14%	10%	5%	2%
women	39%	1%	5%	0.5%
children	10%	23%	39%	12%
boys	8%	18%	38%	18%
girls	11%	5%	40%	17%

Bar Graph



YOUR
DICTIONARY

23 DATA PROTECTION

Data Protection: provides tools and policies to actually restrict access to data. It ensures protection of data from unauthorised access and compromise by external attackers and malicious insiders.

Types of Data Protection

- DATA ENCRYPTION
- DATA BACKUP TO THE CLOUD
- PASSWORD PROTECTION
- IDENTITY AND ACCESS MANAGEMENT (IAM)
- INTRUSION DETECTION AND PREVENTION SOFTWARE
- ENDPOINT PROTECTION — protects gateways to your network, including ports, routers, and connected devices. Endpoint protection software typically enables you to monitor your network perimeter and to filter traffic as needed.
- DATA ERASURE — limits liability by deleting data that is no longer needed.
- DISASTER RECOVERY — a set of practices and technologies that determine how an organization deals with a disaster, such as a cyber attack, natural disaster, or large-scale equipment failure for business continuity



24 DATA PROTECTION (contd.)

Common capabilities of mobile data security solutions include:

- Enforcing communication via secure channels
- Performing strong identity verification to ensure devices are not compromised
- Limiting the use of third-party software and browsing to unsafe websites
- Encrypting data on the device to protect against device compromise and theft
- Perform regular audits of endpoints to discover threats and security issues
- Monitoring for threats on the device and regular vulnerability test
- Setting up secure gateways that can allow remote devices to connect securely to the network

25 RECOMMENDATIONS



- ❖ **Collaboration:** To optimize efficiency and enhance data security in the judiciary system there is need to set up Services Policy and Shared enterprise ICT infrastructure / resources (such as Cloud computing, Database, Customised and integrated Application Software, Computer Devices, Disaster Recovery and Business Continuity facility) for interconnectivity among courts and judicial bodies and relevant agencies.
- ❖ **Adoption of Approved Applications:** The use of the customised solutions like Nigerian Case Management System (NCMS), Legal Mail System, E-filing Application and other Court/Judicial ICT tools to interface with government ministries, agencies and departments that subscribes to court services and to offer self-services to business and citizens
- ❖ **Periodic Upskill of Court Staff:** Court staff should be given consistent and appropriate full-hands trainings, workshops, conferences and seminars regularly for competence

REFERENCES

- Athar Saeed, Jim W. Hall, Jr., “Accelerated Pavement Testing: Data Guidelines.” Washington, DC,2003
- Data Protection and Privacy Committee(DPPC),Storage Networking Association “Why data privacy matters.” 2020 Presentation to the Annual Symposium
- Giovanni Buttarelli, “Data Protection in the Judiciary: The Challenges for Modern Management” Budapest, 24 October 2013
- <https://www.mondaq.com/nigeria/privacy-protection/1183140/data-privacy-and-data-protection-law-in-nigeria>
- <https://www.talend.com/resources/data-privacy/https://www.mondaq.com/nigeria/privacy-protection/1183140/data-privacy-and-data-protection-law-in-nigeria>
- <https://cloud.google.com/learn/what-is-data-governance>
- TMT_DATA_Protection_Survival_Guide_Singles.pdf
- edpb_guidelines_20200420_contact_tracing_covid_with_annex_en(2).pdf
- <https://www.snia.org/education/what-is-data-privacy>
- <https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/>

THANK YOU!

28

QUESTIONS

