NDPC - INTERNATIONAL JOURNAL OF DATA PRIVACY AND PROTECTION

NDPC
NIGERIA DATA PROTECTION COMMISSION

www.ndpc.gov.ng

NDPC – INTERNATIONAL JOURNAL OF DATA PRIVACY AND PROTECTION

NDPC
NIGERIA DATA PROTECTION COMMISSION

The financial support of Switch Solutions is gracefully acknowledged

Switch Solutions

Published by
Nigeria Data Protection Commission

Facebook: @ndpcngr
Twitter: @ndpcngr
Instagram: @ndpcnigeria
LinkedIn: Nigeria Data Protection Commission - NDPC
YouTube: Nigeria Data Protection Commission
Website: www.ndpc.gov.ng

First Published 2025

Printed in Nigeria by
Amatt Brill Impressions Ltd.
Block A2, Suite & Commerce Plaza,
Garki, Abuja.

Table of Contents

Editorial Note

The Nigeria Data Protection Commission (NDPC) was established under the Nigeria Data Protection Act (NDP Act) of 2023. This landmark legislation formalised the Commission's mandate to regulate the processing of personal data and promote initiatives that safeguard the security of personal data and uphold the privacy rights of data subjects.

With the launch of this inaugural edition of the journal, the NDPC embarks on a critical journey to foster dialogue and scholarship on key issues within the evolving data protection ecosystem. This journal aims to serve as a cornerstone for academic and practical insights, encouraging scholarly research that not only deepens knowledge in the field but also provides evidence-based guidance for policymakers and practitioners.

The overarching goal of the journal is to advance innovative research and thought leadership in data privacy and protection. It strives to engage a wide spectrum of stakeholders—academics, industry experts, policymakers, and advocates—toward shaping the future of the data protection ecosystem in Nigeria and worldwide.

This first edition features an array of timely and significant topics, including:

- Navigating Cross-Border Data Transfers and Compliance Challenges: Addressing the complexities and legal frameworks surrounding the global movement of personal data.
- Emerging Technologies for Data Privacy: Artificial Intelligence (AI) and Emerging Technologies: Exploring how cutting-edge technologies can enhance or complicate data privacy frameworks.

- Comparative Analysis of Data Protection Practices Across Regions and Response: Offering insights into how different regions implement and enforce data protection laws.
- Best Practices for Data Breach Prevention strategies to mitigate the risks and impact of data breaches: Highlighting strategies to mitigate the risks and impact of data breaches.
- The Role of Awareness in Promoting Privacy-Conscious Behaviors: Examining how education and awareness campaigns can foster a culture of privacy and responsible data practices.

This journal aspires to become a leading platform for meaningful engagement among experts, researchers, and stakeholders, providing a foundation for collaboration and innovation in the field of data privacy and protection. It is through these conversations and contributions that we can collectively work toward a secure, ethical, and privacy-conscious data-driven future.

Dr. Vincent Olatunji, *CDPO, CPPPS, FIIM*
National Commissioner
Nigeria Data Protection Commission

Implementing a Data Protection Law: The Case of Nigeria

Dr Vincent Olatunji, CPPPS, CDPO, FIIM
National Commissioner/CEO,
Nigeria Data Protection Commission (NDPC)

Abstract

This paper explores the implementation of data protection laws in Nigeria, focusing on the progress, innovations, and challenges since the introduction of the Nigeria Data Protection Act, 2023 (NDP Act). As data protection becomes increasingly vital in the digital age, Nigeria has taken significant steps to safeguard personal information of citizens despite obvious challenges. The paper examines the trajectory leading to the NDP Act, establishment and role of the Nigeria Data Protection Commission (NDPC), and the public-private-partnership model known as the Data Protection Compliance Organization (DPCO). It highlights the achievements of the NDP Act while identifying key hurdles, including legal ambiguities, technological infrastructure gaps, and low public awareness. Finally, the paper provides recommendations to strengthen data protection practices in Nigeria, such as enhancing stakeholder awareness, capacity building, improving legal frameworks, and addressing technological barriers.

Keywords: Nigeria, Data Protection, Nigeria Data Protection Act, DPCO Model, Data Privacy.

1. Introduction

The rapid pace of technological advancements and the exponential growth of data have revolutionized the global landscape, enabling unprecedented innovation and economic development (Wei 2024). This transformation has, however, also brought about pressing challenges particularly concerning the protection of personal data and individual privacy. The volume of data generated globally has surged over the past decade. According to research by Taylor on global development in the use of data, the amount of data generated has dramatically increased from 2 zettabytes in 2010 to 147 zettabytes in 2024, an estimation of 402.89 million terabytes of data each day, with projection exceeding 394 zettabytes by 2028 (Taylor 2024). Given this exponential growth in data generation and processing, maintaining trust, security, and ethical standards while safeguarding personal information becomes major challenges.

In Nigeria, these challenges are particularly significant, given its position as Africa's most populous nation and the 6th most populous nation in the world with over 230 million people. The country's growing population is accompanied by an expanding digital footprint, fueled by widespread internet adoption, with over 134 million internet users according to the Nigerian Communications Commission (NCC), and an increasing reliance on data-driven technologies. Furthermore, Nigeria's economy, which has seen consistent growth, is now primarily powered by the services sector, contributing 58.04% of the GDP in the first quarter of 2023 (Atlasportfolio 2023). This sector thrives on data processing, making a robust data protection law essential for sustained economic growth and the protection of citizens' privacy.

The Nigeria Data Protection Act (NDP Act) of 2023 provides a comprehensive legal framework to address the need to protect the rights, freedom and interest of citizens while ensuring that data protection keeps pace with the rapid technological advancements

and economic shifts. By establishing a comprehensive framework for the lawful, ethical, and secure handling of personal data, the NDP Act aims to safeguard individual rights, foster trust in the digital economy, and position Nigeria as a leader in data governance (King'ori 2023). As the country continues to embrace digital transformation, the effective implementation of the NDP Act will not only enhance privacy and data security but also ensure that Nigeria's economic growth remains inclusive, sustainable, and globally competitive.

2. Data Privacy and Protection

Data privacy and protection refer to the measures taken to safeguard personal data from misuse and unauthorized access, ensuring that individuals' personal information remains private and is processed according to legal and ethical standards (Cloudian, n.d.). In Nigeria, the right to privacy is enshrined in Section 37 of the 1999 Constitution (amended), which guarantees citizens' privacy regarding their homes, correspondence, and communications. This foundational principle supports the right of individuals to have control over their personal information.

Data protection involves technical and organizational measures implemented by individuals or organizations that collect or process data to ensure that personal data is accessible only to authorized users and is used for authorized purposes. Compliance with applicable laws, regulations, and guidelines is crucial for maintaining this level of security (Okorie et al.2024). In Nigeria, data privacy refers to the right of an individual to informational self-determination, as recognized under applicable laws. This fundamental right empowers individuals to control their personal data, aligning with legal frameworks designed to protect privacy and ensure responsible data handling by organizations.

3. Importance of Data Protection Laws

Data protection laws play a critical role in ensuring the ethical, secure, and lawful handling of personal data (Schubert & Barrett 2024). These laws create a robust framework for safeguarding individuals' privacy and promoting trust in data-driven systems. In Nigeria, the implementation of the Nigeria Data Protection Act (NDP Act) underscores the importance of such legislation in addressing the challenges of the digital era. The key benefits of data protection laws include:

1. Privacy Protection: safeguards individuals' personal information, ensuring it is collected, stored, and processed lawfully and transparently.
2. Data Security: enhances mechanisms to prevent data breaches and unauthorized access, fostering a safer digital environment.
3. Trust and Confidence: builds trust between organizations and individuals, encouraging data sharing for legitimate purposes.
4. Legal Accountability: establishes clear legal responsibilities for organizations processing personal data, ensuring adherence to standards.
5. Prevention of Misuse: reduces the risk of unethical practices, such as identity theft, fraud, and data manipulation.
6. Cross-Border Data Flows: facilitates international data transfers by aligning with global standards, thereby enhancing economic opportunities.
7. Transparency: requires organizations to be open about their data processing activities, empowering individuals to make informed decisions.
8. Harmonization with International Standards: promotes alignment with other laws, fostering international cooperation and consistency.
9. Ethical Data Handling: encourages responsible practices in data collection, use, and disposal.

10. Data Economy Growth: strengthens the digital economy by creating a regulatory environment that fosters innovation and trust.

3.1 Foundation of Data Protection Law in Nigeria

The Nigeria Data Protection Act (NDP Act) draws significant influence from international data protection frameworks, particularly those that have set global standards for safeguarding personal information. These global frameworks have not only provided a foundational basis for Nigeria's legislation but have also guided its provisions, ensuring alignment with international best practices.

Global:

1. UN Universal Declaration of Human Rights (1948): Article 12 establishes the right to privacy, providing a universal basis for protecting personal data. The NDP Act reflects this by recognizing data privacy as a fundamental human right.
2. Convention 108 and 108+: The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and its modernized version. Convention 108+ for the protection of individuals with regard to the processing of personal data, have also influenced Nigeria's approach. These agreements prioritize the protection of personal data while facilitating data flows across jurisdictions. Nigeria's NDP Act reflects this focus by balancing data protection with fostering safety in the face of technological advancements.
3. EU Data Protection Directive (1995): Established comprehensive guidelines for protection of individuals with regard to the processing of personal data and on the free movement of such data within the European Union.

4. General Data Protection Regulation (GDPR) (2018): widely regarded as the gold standard for data protection, the GDPR emphasizes principles such as lawful processing, data minimization, purpose limitation, and data subject rights (Regulation 2016/679). These principles are mirrored in the NDP Act, which incorporates similar requirements to ensure transparency, accountability, and fairness in data processing.

Africa:

1. Malabo Convention (2014): The African Union's Convention on Cyber Security and Personal Data Protection, known as the Malabo Convention, encourages African nations to adopt robust data protection laws to facilitate trust, economic integration, and cross-border data flows.
2. African Union Data Policy Framework (2022): A broader initiative encouraging harmonization of data protection standards across the continent to promote economic integration and trust.

West Africa:

ECOWAS Supplementary Act on Personal Data Protection (2010): This regional framework requires Economic Community of West African States (ECOWAS) member states to establish national legal frameworks for the protection of privacy of data relating to the collection, processing, transmission, storage, and use of personal data.

3.2 Data Protection Landscape in Africa

Africa has witnessed significant progress in the adoption of data protection laws, with 37 countries, including Nigeria, enacting leg-

islation to safeguard personal data in an increasingly digital world. These laws vary in robustness and implementation, reflecting the continent's growing recognition of the importance of protecting personal information. Cape Verde led the way as the earliest adopter, enacting its data protection legislation in 2001. More recently, Ethiopia and Malawi joined the trend in 2024, further signaling a heightened awareness and commitment to data protection across Africa.

This gradual but steady adoption signals a growing awareness of the need to align with global data protection standards, ensuring citizens' privacy and fostering trust in the digital economy. As more African nations implement data protection frameworks, the region is positioning itself to better address emerging challenges in cybersecurity, personal data management, and digital innovation.

3.3 Regional Adoption Trends

The African Continental Free Trade Area (AfCFTA) has significantly influenced the adoption of data protection across the African region by fostering cross-border data flows and digital trade. The AfCFTA has necessitated the establishment of harmonized data protection frameworks to ensure trust, security, and compliance in cross-border transactions (Salami, 2022). This has encouraged member states to prioritize the development and implementation of data protection laws, aligning their regulations with regional and international standards to facilitate trade, attract investment, and support innovation.

West Africa

West Africa has emerged as a leader in data protection adoption on the continent. Nigeria, Ghana, and Côte d'Ivoire have implemented comprehensive frameworks that align with regional and

international standards, fostering trust and enabling cross-border data flow.

Southern Africa

Southern Africa showcases a strong legislative presence. South Africa's Protection of Personal Information Act (POPIA) stands out as one of the most comprehensive frameworks on the continent. Similarly, Zambia's Data Protection Act provides robust measures to protect personal data.

East Africa

East Africa presents a mixed landscape. Kenya has developed a robust data protection framework, which serves as a model for the region. Other countries, however, are at various stages of developing or implementing their laws.

Central Africa

Central Africa lags in the adoption of data protection legislation. Only a few countries, such as Chad and Gabon, have enacted laws, leaving significant gaps in the region's data governance.

North Africa

Several North African countries, including Morocco and Tunisia, have established comprehensive data protection frameworks.

Unregulated Jurisdictions

Despite the progress made, 17 African countries, including Cameroon, Mozambique, Namibia, and the Democratic Republic of Congo, still lack formal data protection laws. This legislative gap pos-

es risks to privacy and data security, especially as these countries experience increased internet penetration and data-driven activities.

4. Enabling Policies, Laws, and other Instruments Guiding NDPC's Activities

The Nigeria Data Protection Commission (NDPC) operates within a framework of policies, laws, and instruments designed to ensure comprehensive data protection and compliance across various sectors. These tools provide the foundation for the Commission's activities and regulatory enforcement.

Nigeria Data Protection Act (NDP Act) 2023

Enacted on June 12, 2023, the NDP Act is a landmark legislation aimed at regulating the processing of personal data and safeguarding individuals' privacy rights in Nigeria. The act addresses challenges posed by emerging technologies and strengthens legal frameworks for data protection.

Nigeria Data Protection Regulation (NDPR) 2019

The NDPR serves as Nigeria's foundational data protection regulation, establishing guidelines for the processing of personal data and setting the stage for subsequent legal developments in data privacy. The NDPR Implementation Framework outlines the practical steps for compliance and enforcement of the regulation.

Service-Wide and Institutional Compliance Instruments

1. Service-Wide Compliance Directive (Ref. No. SGFI-OPIIIS.3/Xl/186): Issued on November 7, 2022, to ensure

uniform adherence to NDPR provisions across government agencies.

2. HOS Guidelines (16 Nov., 2022): Complementary guidance from the Head of Service to promote institutional compliance with data protection standards.

Strategic Framework and Guidelines

1. Nigeria Data Protection Strategic Roadmap and Action Plan 2023 - 2027: A comprehensive document outlining the strategic direction for data protection governance in Nigeria.
2. Code of Conduct for Data Protection Compliance Organizations (DPCOs): Provides ethical and operational guidelines for DPCOs.
3. Guidance Notice: Details the requirements for the registration of data controllers and data processors of major importance, ensuring a robust compliance mechanism.
4. General Application and Implementation Directive (GAID) for the Nigeria Data Protection Act (NDP Act): outlines the scope of the NDP Act and provides guidance on personal data processing especially for data controllers/processors and specifies the categories of data subjects covered.

5. Summary of the Nigeria Data Protection Act 2023

The Nigeria Data Protection Act 2023, signed into law by President Bola Ahmed Tinubu, GCFR, is the most comprehensive legal instrument guiding the NDPC's activities. It consists of 12 parts that collectively form the backbone of data protection governance in Nigeria.

Rights of Data Subjects

The Nigeria Data Protection Act, 2023, aims to safeguard the rights, freedoms, and interests of data subjects, reinforcing their control over personal data (Babalola & Balboni, 2023). These rights are anchored in Section 37 of the Constitution of the Federal Republic of Nigeria, 1999 (as amended), which guarantees the privacy of citizens. Among these rights is the right to be informed, ensuring individuals are notified about the collection, processing, and purpose of their data. Similarly, the right to access allows individuals to review their data held by organizations, while the right to rectify ensures corrections to inaccuracies or incomplete information.

Moreover, individuals have the right to data portability, enabling seamless transfer of data between service providers. The right to be forgotten empowers individuals to request the deletion of their data when no longer necessary. Data subjects can also invoke the right to restrict processing, limiting how their data is handled in specific contexts. The right to object to processing, particularly for purposes such as direct marketing, further underscores individual control. Data subjects also have the right not to be subjected to automated decision-making, ensuring decisions affecting them are not made solely by automated systems without human intervention. Lastly, individuals have the right to complain to the Nigeria Data Protection Commission (NDPC), ensuring grievances can be formally addressed.

Principles of Personal Data Processing

The Nigeria Data Protection Act, 2023, establishes key principles to guide the handling of personal data, ensuring fairness, security, and accountability. A core principle is lawfulness, fairness, and transparency, which demands that data processing is carried out in a manner that is not only legal but also fair and open to scrutiny. Purpose limitation ensures that personal data is collected and

used solely for specific, legitimate objectives and not for unrelated purposes.

Another foundational principle, data minimization, mandates that only the data necessary for a particular purpose should be collected. The principle of accuracy emphasizes the importance of maintaining correct and up-to-date information, reducing risks associated with errors. Additionally, integrity and confidentiality focus on implementing robust security measures to safeguard data against unauthorized access, loss, or damage. Lastly, the principle of storage limitation requires that personal data is not retained longer than necessary for the intended processing purposes.

Lawful Basis of Data Processing

The NDP Act, 2023, outlines specific lawful bases for processing personal data, ensuring compliance with legal and ethical standards. One key basis is consent, where individuals explicitly authorize the use of their data. Data may also be processed to fulfill contractual obligations, such as providing services agreed upon with a data subject. Another lawful basis, legal obligation, mandates data processing to comply with applicable laws or regulations.

In cases involving vital interests, data processing may occur to protect someone's life or wellbeing. Public interest represents another lawful basis, permitting data use to promote the common good, such as in public health or governance. Finally, legitimate interests allow data processing to support legitimate business objectives, provided these do not conflict with the rights and freedoms of individuals.

Application and Scope of the Nigeria Data Protection Act (NDP Act)

The Nigeria Data Protection Act (NDP Act) applies broadly to ensure comprehensive coverage of data processing activities involving Nigerian data subjects. It governs any data controller or processor domiciled, resident, or operating within Nigeria, as well as situations where the processing of personal data occurs within Nigeria, irrespective of the location of the data controller or processor.

Additionally, the Act extends to data controllers or processors not domiciled, resident, or operating in Nigeria but processing the personal data of individuals in Nigeria. This extraterritorial application aligns with global data protection trends, emphasizing the protection of Nigerian data subjects irrespective of where their data is processed.

Why Compliance Matters

Compliance with the NDP Act is critical for organizations operating within Nigeria or handling the personal data of Nigerian citizens. Beyond fulfilling legal obligations, adherence to the Act fosters trust and confidence, signaling a commitment to ethical and responsible data management. This trust is essential in maintaining positive relationships with customers, stakeholders, and the public.

Non-compliance carries significant risks, including substantial fines, legal consequences, and irreparable harm to an organization's reputation. Moreover, compliance ensures global competitiveness, as adherence to robust data protection standards becomes increasingly vital in a world where data privacy regulations are evolving rapidly. Organizations that prioritize compliance not only protect their operations but also enhance their long-term sustainability in the global market.

6. Mandate and Functions of the Nigeria Data Protection Commission (NDPC)

The Nigeria Data Protection Commission (NDPC) is the authoritative body entrusted with enforcing the Nigeria Data Protection Act, 2023 and administering all data protection matters across Nigeria. Its primary mandate is to safeguard the privacy rights of individuals and ensure that data processing activities are carried out lawfully and ethically. The NDPC executes several critical functions, including:

i. Regulation: Establishing rules and guidelines for lawful data processing in line with the NDP Act.
ii. Development of Privacy-Enhancing Technologies: Promoting innovation in technologies that uphold privacy.
iii. Accreditation and Registration: Accrediting and maintaining a register of Data Protection Compliance Organizations (DPCOs).
iv. Registration of Data Controllers and Processors: Ensuring data handlers meet statutory requirements.
v. Awareness Creation: Educating the public and stakeholders on data protection rights and obligations.
vi. Complaint Handling: Providing mechanisms for individuals to report breaches or violations.
vii. Compliance Monitoring: Conducting audits and inspections to ensure adherence to the NDP Act.
viii. International Engagement: Fostering global partnerships to align Nigeria with international data protection standards.

7. Strategic Roadmap and Action Plan

The Nigeria Data Protection Commission operates using a Strategic Roadmap and Action Plan (NDP-SRAP) designed to steer the data protection ecosystem toward sustainable development. This framework emphasizes optimizing opportunities for growth, en-

suring regulatory efficiency, and enhancing the well-being of Nigerian citizens through data protection initiatives.

The NDP-SRAP is built on five key pillars:

1. Governance: Strengthening institutional structures and processes for effective data protection.
2. Human Capital Development: Building capacity and expertise within the ecosystem.
3. Ecosystem and Technology: Leveraging innovative technologies to support privacy and data security.
4. Collaboration and Cooperation: Encouraging partnerships between public, private, and international entities.
5. Funding and Sustainability: Ensuring financial resilience to achieve long-term objectives.

These pillars align with the eight priorities of the President of the Federal Republic of Nigeria and the five pillars of the Federal Ministry of Communications, Innovations, and Digital Economy. Together, they demonstrate the NDPC's commitment to positioning Nigeria as a global leader in data protection and digital governance.

8. The DPCO Model

The Data Protection Compliance Organization (DPCO) model is a hallmark of the Nigeria Data Protection Regulation (NDPR) 2019 Implementation Framework, leveraging a Public-Private Partnership (PPP) approach. This model empowers private sector organizations, licensed as DPCOs, to support the enforcement and compliance of data protection regulations in Nigeria.

Key Features of the DPCO Model:

1. Licensing: DPCOs are licensed entities authorized to deliver a broad range of services aimed at ensuring compliance with data protection standards.
2. Compliance Services: These organizations are pivotal in guiding data controllers and processors to align their operations with regulatory requirements.

Core Activities:

1. Registration of Data Controller/Processor.
2. Training and awareness.
3. Conducting DPIAs.
4. Conducting audits to evaluate data protection measures.
5. Filing annual audit reports with the Nigeria Data Protection Commission (NDPC).

Achievements Under the DPCO Model:

1. Licensed DPCOs: the NDPC has licensed 243 DPCOs across various sectors.
2. Audit Filings: As at December 2024, 8,142 audit filings have been submitted, reflecting a significant commitment to data protection compliance across organizations.

9. Key Programmes, Projects, and Initiatives

The Nigeria Data Protection Commission (NDPC) is actively driving several programs and initiatives to ensure the effective implementation of the Nigeria Data Protection Act (NDP Act) and promote a robust data protection ecosystem. These include:

1. Data Processor/Controller Registration: A structured system for the registration of data handlers in Nigeria.

2. National Data Protection Officer Certification System: Certifying professionals to meet global standards in data protection practices.
3. Responsible Data Management Course for Public Sector Officers: Equipping public servants with knowledge of ethical data management.
4. National Privacy Week: A dedicated time to raise awareness about data protection and privacy rights.
5. Capacity Building Program: Enhancing the skills of Data Protection Officers (DPOs) and other stakeholders.
6. Partnership and Collaboration: Fostering cooperation with local and international stakeholders.
7. Awareness Campaigns: Educating individuals and organizations on their rights and responsibilities under the NDP Act.
8. Data Protection Compliance Organizations (DPCOs): Accrediting entities to monitor and ensure compliance.
9. Adopt-a-School Initiative: Promoting data protection awareness among students and educational institutions.
10. Code4Privacy Hackathon: Encouraging innovation in developing privacy-enhancing technologies.

9.1 Key Achievements

The NDPC has made significant strides since its establishment, with notable milestones that underscore its dedication to advancing data protection in Nigeria.

1. Governance
   i. Signing of the Nigeria Data Protection Act into law (12 June 2023).
   ii. Launching the Nigeria Data Protection Strategic Roadmap and Action Plan (December 2023).

iii. Resolution by the National Council on Communications and Digital Economy (NCCDE) enforcing compliance with the NDP Act (8 December 2023).
iv. Federal Government Circular mandating MDAs to adhere to NDPR (7 November 2022).
v. Service-wide Guidelines for Personal Information Technology Devices making compliance mandatory in public service (16 November 2022).

2. Human Capital

i. Trained over 1,500 Data Protection Officers in both public and private sectors.
ii. Conducted over 140 training programmes with over 55,000 beneficiaries.
iii. Creation of over 30,123 new jobs for professionals in the ecosystem.
iv. Licensed the Institute of Information Management (IIM) to certify data protection professionals.
v. Ongoing certification process for 500 Data Protection Officers.

3. Collaboration and Cooperation

i. Engaged over 120 major data controllers, including the Federal Ministry of Health, Central Bank of Nigeria, and National Identity Management Commission.
ii. Inaugurated the National Data Protection Adequacy Programme (NaDPAP) on 22 September 2022.
iii. Admission to the Global Privacy Assembly (October 2023).
iv. Membership in the Network of African Data Protection Authorities (NADPA).
v. Won the hosting right for the NADPA 10th AGM & Conference which will hold in May,2025.

vi. Collaborative engagements with Data Protection Authorities in Ghana, Kenya, the UK, Canada, Finland, the U.S., and Singapore, leading to an ongoing MOU with the UK ICO.

vii. Signed MOUs on data protection with entities such as the Federal Ministry of Youth Development, National Insurance Commission (NAICOM), Federal Competition and Consumer Protection Commission (FCCPC), Nigeria Lottery Commission (NLRC), Small and Medium Enterprises Development Agency of Nigeria (SMEDAN), Huawei Technologies, Office of the Privacy Commissioner of Canada (OPCC), and the Dubai Financial Centre Authority (DIFCA).

4. Funding and Sustainability

i. Economic and Employment Contributions: The data protection sector has generated ₦16.2 billion in revenue within four years.

10. NDPC Statistics

The Nigeria Data Protection Commission (NDPC) continues to record significant progress in its efforts to safeguard data privacy and ensure compliance with the Nigeria Data Protection Act (NDP Act) 2023. Below are highlights of the Commission's recent statistics:

i. Investigations: The NDPC has investigated over 20 cases across various sectors, demonstrating its commitment to enforcing compliance and addressing data protection breaches. Sectors under investigation include Finance, Technology, Government, Logistics, Education, Consulting, Gaming/Lottery

ii. Complaints and Compliance Monitoring: The Commission has received over **4,500** complaints, highlighting the grow-

ing awareness and active engagement of individuals and organizations in upholding data protection rights.

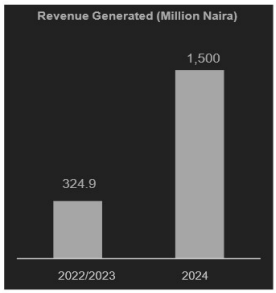
iii. Audit Filings: Registered Data Controllers and Processors have submitted over **8,142** audit filings to the Commission, indicating widespread efforts to meet compliance standards.

iv. Ecosystem Growth: The Nigerian data protection ecosystem has generated over **N16.2 billion**, showcasing its potential as a thriving and sustainable sector.

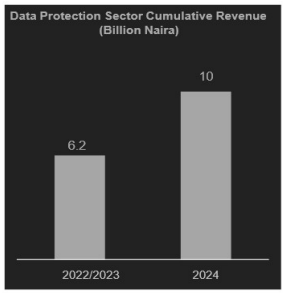
v. Registered Data Controllers/Processors of Major Importance: The Commission has registered **33,052** Data Controllers and Processors categorized as having significant importance, ensuring tighter oversight on key stakeholders.

vi. Registered Data Protection Officers (DPOs): Over **7,213** DPOs have been registered, equipping organizations with skilled personnel to navigate and implement data protection protocols effectively.

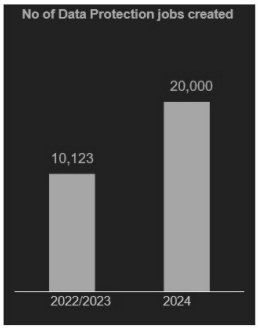
Ecosystem Growth



Revenue Generated by the Commission
2022/2023: 324,925,351.00
2024: 1,500,000.00
Total: 1,834,925,351.00

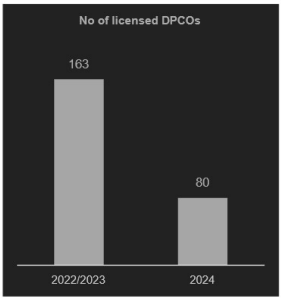


Data Protection Sector Cumulative Revenue
2022/2023: 6,200,000,000.00
2024: 10,000,000,000.00
Total:16,200,000,000.00

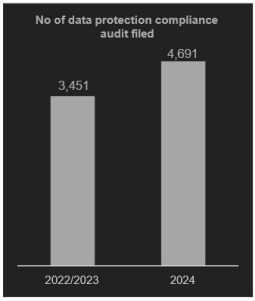


No of Data Protection jobs created
2022/2023: 10,123
2024: 20,000
Total: 30,123

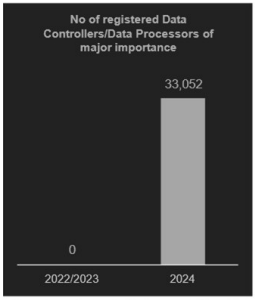
Compliance



No of licensed DPCOs
2022/2023: 163
2024: 80
Total: 243

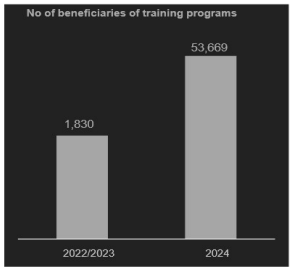


No of data protection compliance audit filed
2022/2023: 3,451
2024: 4,691
Total: 8,142



No of registered Data Controllers/Data Processors of major importance
2022/2023: 0
2024: 3,052 DCs + 30,000 MNO Agents
Total: 33,052

No of training programs conducted
2022/2023: 55
2024: 87
Total: 142



No of beneficiaries of training programs
2022/2023: 1830
2024: 53,699
Total: 55,529

11. Challenges

Despite the progress made by the Nigeria Data Protection Commission (NDPC) in advancing data protection initiatives, several challenges remain in the effective enforcement of data privacy laws. These challenges include:

1. Lack of Awareness and Education

   One of the major obstacles to data protection in Nigeria is the lack of widespread awareness and education about data privacy rights and obligations. Many organizations, as well as individuals, are still unaware of their roles and responsibilities under the Nigeria Data Protection Act (NDP Act), making it difficult to foster a culture of compliance.

2. Recruiting, Training, and Retention of Qualified Personnel

   There is a shortage of data protection experts in the country, which makes recruitment, training, and retention of qualified data protection officers (DPOs) and cybersecurity professionals a persistent challenge. Skilled personnel are in high demand globally, and Nigeria faces competition from both domestic and international organizations looking to hire top talent.

3. Limited Resources

The NDPC, like many regulatory bodies, faces resource constraints that affect its ability to fully implement and enforce the NDP Act. Limited human, financial, and technical resources hinder the Commission's capacity to conduct widespread inspections, investigations, and capacity-building initiatives.

4. Rapid Technological Advancements

The rapid pace of technological advancements presents a significant challenge for data protection regulation. Emerging technologies, such as artificial intelligence, big data analytics, and the Internet of Things (IoT), create new vulnerabilities in personal data processing, which require the continuous adaptation of policies and enforcement mechanisms.

5. Balancing Innovation and Regulation

Striking the right balance between encouraging innovation and ensuring data protection is a complex challenge. While it is essential to promote technological development, it is equally important to implement regulations that protect individuals' privacy rights and prevent data misuse.

6. Enforcement and Compliance

Ensuring compliance with the NDP Act remains a significant challenge, particularly in sectors where there is a lack of understanding or reluctance to comply with data protection laws. Enforcement of penalties for non-compliance is also hindered by the need for more robust mechanisms and legal frameworks.

7. Cybersecurity Threats

   As the digital landscape grows, cybersecurity threats continue to increase. Cyberattacks and data breaches can compromise the integrity of personal data, posing serious risks to individuals' privacy rights. Strengthening cybersecurity measures and ensuring data protection are critical to safeguarding personal information.

12. Conclusion

In conclusion, the NDPC's efforts are integral to the development of a trustworthy, secure, and sustainable data protection environment in Nigeria, positioning the country as a leader in data protection and privacy within Africa and on the global stage. Through the Nigeria Data Protection Act (NDP Act) 2023, the Commission has established a comprehensive regulatory framework that balances innovation with privacy, ensuring that individuals' rights are protected while supporting the country's digital transformation. The Commission's key achievements reflect its commitment to fostering a robust data protection ecosystem.

However, the journey ahead remains complex. The NDPC continues to face challenges such as limited resources, a need for greater public awareness, rapid technological advancements, and evolving cybersecurity threats. These obstacles underscore the importance of continued collaboration, capacity building, and investment in both human capital and technological infrastructure. Moving forward, the NDPC's success will depend on its ability to address these challenges while maintaining its focus on its mission to protect individuals' data rights, promote compliance across all sectors, and foster global cooperation. With continued support and a focus on innovation, the NDPC will play a crucial role in shaping Nigeria's data privacy future.

Works Cited

Babalola & Balboni. Annonated Nigeria Data Protection Act, 2023. Noetico Repertum Inc, 2023.

Data Protection Africa. "Which African countries have a data protection law?" dataprotection.africa/which-african-countries-have-a-data-protection-law/

Industry Statistics. Nigerian Communications Commission. 2024. https://www.ncc.gov.ng/statistics-reports/industry-overview.

King'ori Mercy. Nigeria's New Data Protection Act, Explained. Nigeria's New Data Protection Act, Explained - Future of Privacy Forum. 2023.

Okorie et al. Ethical Considerations in Data Collection and Analysis: a Review: Investigating Ethical Practices and Challenges in Modern Data Collection and Analysis. International Journal of Applied Research in Social Sciences. 6. 1-22. 10.51594/ijarss.v6i1.688, 2024.

Salami Emmanuel. Implementing the AfCFTA Agreement: A Case for the Harmonization of Data Protection Law in Africa. Journal of African Law. 2022;66(2):281-291. doi:10.1017/S0021855322000110

Schubert, K.D., Barrett, D. Data Governance, Privacy, and Ethics. In: Lacity, M.C., Coon, L. (eds) Human Privacy in Virtual and Physical Worlds. Technology, Work and Globalization. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-51063-2_5. ,2024.

Taylor Petroc. Volume of data/information created, captured, copied, and consumed

worldwide from 2010 to 2023, with forecasts from 2024 to 2028, Statista, 2024.

www.statista.com/statistics/871513/worldwide-data-created/

Wei, Xing. Data-Driven Revolution: Advancing Scientific and Technological

Innovation in Chinese A-Share Listed Companies. J Knowl Econ 15, 9975–10002,

2024. https://doi.org/10.1007/s13132-023-01476-6.

AI and Data Privacy in the Internet of Things (IoT): A New Frontier in the Connected World

Immaculeta Chidera Onyekwe
Data Privacy Analyst

Abstract

In recent years, the rapid expansion of the Internet of Things (IoT) has brought unprecedented opportunities for innovation, while also raising significant concerns about data privacy and protection. In the connected world of IoT, vast amounts of personal data are collected, transmitted, and processed through AI-powered systems. These interconnected devices, coupled with AI, allow for enhanced consumer targeting, decision-making, and automation. However, these advancements also escalate risks, as AI models often process large datasets in ways that are complex to regulate. Embedded AI systems in IoT environments can inadvertently infringe on privacy rights by gathering sensitive personal information from diverse sources or utilizing data in ways that exceed individuals' privacy expectations.

This paper examines the challenges AI poses to data privacy within IoT ecosystems, highlighting the critical need to balance technological benefits with robust privacy safeguards. It further explores potential measures organizations and regulators can implement to protect data in this rapidly evolving landscape. Ultimately, the paper advocates for a harmonized approach that leverages the transformative power of AI in IoT while safeguarding in-

dividuals' privacy rights and fostering ethical innovation.

Keywords: Internet of Things (IoT), Artificial Intelligence (AI), Data privacy, Safeguards, Regulation.

1. Introduction

In the rapidly evolving digital landscape, the Internet of Things (IoT) is revolutionizing the way devices, systems, and individuals interact, creating a seamlessly connected world. At the heart of this ecosystem lies personal data, now frequently termed the "new currency" of the digital economy (Zuboff). As billions of interconnected devices—from smartphones to smart homes—continuously collect and transmit data, the volume of information available for analysis has surged exponentially (Kshetri 32). This unprecedented scale of data collection offers significant opportunities for innovation and efficiency, particularly when harnessed by Artificial Intelligence (AI) systems (Brynjolfsson and McAfee).

AI, with its capacity to process and analyze vast datasets in real-time, has emerged as a key enabler within the IoT ecosystem (Arntz, Melanie, et al. 5). It allows platforms to derive insights, predict behaviors, and automate decisions with a precision that was previously unimaginable (Calo 399). However, while AI promises to unlock new capabilities and optimize IoT functionalities, it also introduces serious concerns regarding data privacy. The ability of AI to infer, aggregate, and reclassify non-personal data into identifiable personal information raises ethical and legal challenges, particularly around the protection of individuals' privacy rights (Solove).

As AI continues to evolve, there is growing recognition that existing data protection laws and privacy frameworks may be insufficient to address the complexities of AI-driven IoT environments (Tufekci). The interconnectivity between AI and IoT intensifies vulnerabilities related to data security and personal information handling (Greenleaf 10). This confluence of technologies demands a rethinking of regulatory approaches to ensure that while innovation thrives, the privacy and autonomy of individuals remain safeguarded.

In this paper, the intersection of AI, IoT, and data privacy will be explored, with a particular focus on the regulatory challenges that emerge in this new frontier of the connected world. The aim is to examine how AI's role in IoT exacerbates privacy risks and to discuss potential safeguards that can ensure a balanced, secure, and competitive digital environment (Gellman and Schwartz).

2. Overview of Artificial Intelligence (AI) and the Internet of Things (IoT)

AI and IoT are two pivotal technologies transforming the digital world. Artificial Intelligence (AI) refers to the simulation of human intelligence in machines, enabling them to perform tasks such as decision-making, learning, and pattern recognition autonomously. AI spans various technologies, including machine learning, deep learning, and natural language processing (NLP), offering significant advancements in automation, data analysis, and predictive modeling. The Internet of Things (IoT) refers to a network of interconnected devices, often embedded with sensors, software, and other technologies, that collect and exchange data with other devices or systems over the internet (Smith).

The integration of AI into IoT creates a synergistic relationship that enhances automation, decision-making, and operational efficiency. For instance, IoT devices, such as smart home systems or

industrial sensors, generate massive amounts of data, while AI algorithms process this data to derive actionable insights, such as predictive maintenance, energy optimization, and user behavior prediction (Garcia 112). This convergence has found widespread applications in various sectors, including healthcare, transportation, and smart cities (Brown 45).

AI's role in IoT is not just limited to data processing; it enables IoT devices to become more intelligent and autonomous, reducing human intervention and facilitating real-time, data-driven decisions. As a result, AI-powered IoT systems have enhanced the capability of managing complex systems in real-time and at scale, making AI an indispensable component in the future of IoT development (Johnson 87).

2.1 Data Privacy Risks in AI-IoT Integration

The integration of AI and IoT raises significant data privacy risks due to the continuous collection, processing, and sharing of large amounts of personal and non-personal data. As IoT devices become ubiquitous, they gather data from a wide range of sources, including personal devices, wearables, and smart home systems, raising concerns about user consent and data ownership (Williams). AI algorithms further exacerbate these concerns by enabling the aggregation and re-identification of anonymized data (Miller 98).

One of the primary privacy challenges in AI-IoT integration is data aggregation, where AI systems combine data from various IoT devices to generate detailed profiles of individuals, potentially without their consent. For example, data from fitness trackers, smart refrigerators, and security cameras could be aggregated to reveal intimate details about a person's lifestyle, habits, or health status, even if each individual device collects only limited information (Taylor 76). This raises questions about informed consent, as most

users are not fully aware of how their data is being collected, processed, and shared across platforms (O'Connell 65).

Additionally, AI-powered IoT systems can introduce biases into automated decision-making processes. If AI models are trained on biased or incomplete data, they can perpetuate or amplify biases, leading to discriminatory outcomes in sectors such as healthcare, finance, or employment (Karim 34). Furthermore, the sheer scale of IoT networks makes it challenging to ensure cybersecurity across all devices, leaving them vulnerable to hacking, data breaches, and unauthorized access (Patel 101).

2.2 Legal and Ethical Considerations in AI-IoT Ecosystems

The integration of AI with IoT brings forth numerous legal and ethical challenges, especially regarding data privacy, accountability, and transparency. Current data protection frameworks, such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Nigeria Data Protection Act (NDPA), impose restrictions on data collection and processing, but they fall short when addressing the complexities introduced by AI and IoT (Nwogu).

One significant legal issue is the lack of transparency in AI algorithms, often referred to as the "black box" problem. AI models used in IoT systems are frequently complex and opaque, making it difficult for users, developers, and regulators to understand how decisions are made. This raises ethical concerns about accountability, as it is unclear who should be held responsible when AI-driven IoT devices cause harm or make erroneous decisions (Barnes 14). For example, if an AI-powered IoT device misdiagnoses a medical condition based on faulty data, determining accountability becomes challenging (Williams 76).

Moreover, the ownership of data collected by IoT devices is another pressing issue. While users generate vast amounts of data

through their interactions with IoT systems, large digital platforms (LDPs) often claim ownership of this data, leading to potential conflicts regarding how it is used, shared, or sold (Tunde 53). The Nigeria Data Protection Act (NDPA) emphasizes the right to data privacy and requires organizations processing personal data to adhere to lawful, fair, and transparent practices. However, similar to GDPR and CCPA, the NDPA struggles to provide clarity on data ownership and user control over personal data in AI-IoT systems (Lee 45).

Ethically, the use of AI in IoT ecosystems raises concerns about the fairness and biases inherent in AI models. IoT devices collect data from diverse populations, but if AI systems are trained on biased or incomplete data sets, the decisions made by these systems could reinforce existing inequalities. For instance, AI systems used in predictive policing or healthcare could disproportionately target or neglect certain demographic groups (Ahmed 112).

2.3 Regulatory Challenges and Gaps in AI-IoT Systems

Despite existing regulations, significant gaps persist in addressing the unique challenges posed by the integration of AI and IoT. The global nature of IoT networks presents challenges for regulatory bodies, as data collected by IoT devices often crosses borders, subjecting it to different legal jurisdictions with varying levels of data protection (Chan 23). For example, while GDPR provides stringent data protection rules within the European Union, its enforcement becomes complicated when IoT devices send data to regions without similar data protection standards, such as countries with less mature data privacy laws (Emmanuel 54).

Another challenge is the rapid evolution of AI and IoT technologies, which often outpaces the development of regulatory frameworks. Current laws may not fully account for the intricacies of how AI processes and re-identifies data collected by IoT devices, leading to loopholes in data privacy protection (Roberts 80). For

instance, IoT devices may collect non-personally identifiable information (PII), but AI algorithms can aggregate this data to re-identify individuals, circumventing traditional privacy safeguards (Zhao 94).

Data minimization principles, which require organizations to collect only the data necessary for a specific purpose, are also difficult to enforce in AI-IoT ecosystems, where vast amounts of data are needed for training AI models. This creates a conflict between the need for innovation and the protection of user privacy, as excessive data collection could increase the risk of data breaches or misuse (Adewale 23).

To address these gaps, experts propose the development of AI-specific legal frameworks that focus on issues such as algorithmic accountability, transparency, and data fairness. In addition, international agreements on cross-border data transfers and standardized IoT security certifications are being considered to ensure consistent data protection across regions (Park, 16).

3. Proposed Safeguards for Balancing Innovation and Privacy in AI-IoT Systems

In light of the privacy risks posed by AI-IoT integration, it is critical to implement safeguards that strike a balance between technological innovation and the protection of individual privacy rights. One approach is to adopt the principle of Privacy by Design, which requires that data protection measures be integrated into the development process of IoT devices and AI systems from the outset (Anderson 68).

Data anonymization and pseudonymization are also essential techniques for protecting user privacy while allowing organizations to harness IoT data for analysis. These methods involve removing or obfuscating personally identifiable information, thus minimizing the risk of data breaches or misuse. However, AI's abil-

ity to re-identify anonymized data remains a concern, highlighting the need for more robust privacy safeguards (Bashir 33).

Algorithmic transparency is another critical safeguard. Developers of AI systems should be required to provide explanations of how their models work, ensuring that users and regulators can understand the rationale behind decisions made by AI-powered IoT devices. This would not only foster greater trust in AI systems but also facilitate better oversight and accountability (Silva 11).

Finally, implementing strong cybersecurity measures is essential to safeguard IoT networks from unauthorized access and data breaches. Techniques such as multi-factor authentication, encryption, and regular security updates should be employed to protect AI and IoT systems from potential threats (Nwosu 23).

4. Future Trends in AI, IoT, and Data Privacy

1. Evolution of AI Technologies: As AI continues to advance, we are witnessing a surge in more sophisticated models and algorithms. These include enhancements in deep learning, reinforcement learning, and explainable AI (XAI) (Smith). Future AI systems are expected to achieve greater autonomy and efficiency, learning from minimal data while providing more accurate predictions and personalized experiences (Brown 45). The integration of AI with IoT will enable real-time data processing and decision-making, driving innovations in smart cities, autonomous vehicles, and industrial automation (Johnson 87).

2. Expansion of IoT Ecosystems: The IoT landscape is rapidly expanding with the proliferation of connected devices. Future trends indicate a move towards more seamless and interoperable IoT ecosystems. Advances in edge computing and 5G technology are expected to enhance IoT performance by reducing latency and increasing data transfer speeds (Garcia 112). Additionally, IoT devices are becoming more intelligent, incorporating AI to analyze

and respond to data locally, thus reducing dependency on centralized cloud servers (Lee 45).

3. Enhanced Data Privacy Measures: With increasing concerns over data breaches and misuse, future data privacy frameworks are anticipated to incorporate more robust measures. Innovations include the adoption of privacy-enhancing technologies (PETs) such as homomorphic encryption, secure multiparty computation, and differential privacy (Patel 101). These technologies aim to protect data during processing and ensure compliance with stringent privacy regulations (Taylor 76). The evolving landscape of data privacy will also see a greater emphasis on user consent and transparency, driven by regulations like the GDPR and emerging standards (Chan 23).

4. Regulatory and Ethical Considerations: As AI and IoT technologies evolve, so too will the regulatory landscape. Governments and organizations are expected to develop more comprehensive policies addressing the ethical use of AI, data protection, and the rights of individuals in a connected world. This includes updating data protection laws to address new challenges posed by AI and IoT, ensuring that privacy concerns are adequately addressed while fostering innovation (Zhao 94).

5. Integration of AI and IoT in Emerging Applications: Future applications of AI and IoT are likely to revolutionize various sectors, including healthcare, finance, and transportation. AI-driven IoT solutions will enhance predictive maintenance, personalized medicine, and smart infrastructure, leading to more efficient and adaptive systems (Roberts 80). For instance, in healthcare, AI-powered IoT devices will enable real-time health monitoring and predictive analytics, improving patient outcomes and operational efficiencies (Barnes 14).

5. Conclusion

As the landscape of digital technology continues to evolve, the intersection of artificial intelligence (AI) and the Internet of Things (IoT) represents a pivotal frontier in the connected world. The integration of AI with IoT technologies is not only transforming industries but also reshaping how personal data is collected, processed, and protected. This paper has explored the profound implications of these advancements on data privacy and protection, highlighting both the opportunities and challenges that lie ahead.

The rapid development of AI has endowed IoT systems with unprecedented capabilities for real-time data processing, predictive analytics, and personalized user experiences. However, these advancements come with significant privacy risks. The aggregation and analysis of vast amounts of personal data by large digital platforms (LDPs) can lead to increased exposure of sensitive information and potential breaches of privacy. The shift towards more intelligent and autonomous IoT devices further complicates the data protection landscape, necessitating robust and adaptive privacy frameworks.

The study has underscored the importance of balancing technological innovation with the protection of individual privacy rights. Regulatory measures, such as the General Data Protection Regulation (GDPR) and the Nigeria Data Protection Act (NDPA), play a crucial role in addressing these challenges. Yet, as AI and IoT technologies continue to advance, existing regulations may need to be updated to address new privacy concerns and technological realities.

Future trends in AI and IoT indicate a continued expansion of connected ecosystems and more sophisticated data processing capabilities. This evolution will likely drive further innovations across various sectors but will also necessitate ongoing vigilance in data privacy and security. Emerging technologies, such as pri-

vacy-enhancing techniques and improved consent mechanisms, offer promising avenues for enhancing data protection while fostering technological progress.

In conclusion, the integration of AI and IoT presents both remarkable opportunities and substantial risks. To navigate this complex landscape, it is essential for stakeholders—regulators, technologists, and consumers—to collaborate in developing and implementing effective privacy measures. Ensuring that advancements in AI and IoT do not come at the expense of individual privacy will be crucial in achieving a secure and equitable digital future.

Works Cited

Adewale, Funmi. "Cybersecurity in AI-IoT Systems: Emerging Threats and Safeguards." Nigeria Tech Journal, vol. 7, no. 2, 2024, pp. 23-45.

Ahmed, Sofia. "Algorithmic Fairness: Challenges in AI Systems for IoT Devices." Ethical AI Review, vol. 8, no. 3, 2023, pp. 112-128.

Anderson, Richard. "Privacy by Design in AI-IoT Development: A Best Practices Guide." IoT Privacy Review, vol. 11, no. 3, 2024, pp. 68-85.

Arntz, Melanie, et al. "The Risk of Automation for Jobs in OECD Countries: A Comparative Analysis." OECD Social, Employment and Migration Working Papers, no. 189, 2016, pp. 5–40.

Barnes, Michael. "Black Box Algorithms in IoT Systems: Legal and Ethical Issues." Journal of Technology and Society, vol. 16, no. 1, 2023, pp. 14-33.

Bashir, Khalid. "The Threat of AI Re-identification in IoT Systems." Cybersecurity and AI Journal, vol. 10, no. 2, 2024, pp. 33-49.

Brown, Emily. "Natural Language Processing in IoT Devices: Applications and Challenges." Journal of AI Applications, vol. 11, no. 3, 2023, pp. 45-67.

Brynjolfsson, Erik, and Andrew McAfee. "The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies". W.W. Norton & Company, 2014.

Calo, Ryan. "Artificial Intelligence Policy: A Primer and Roadmap." Utah Law Review, vol. 2017, no. 5, 2017, pp. 399-419.

Chan, Victor. “Cross-Border Data Transfers in IoT Systems: Regulatory Gaps and Solutions.” International Journal of Data Privacy, vol. 6, no. 1, 2024, pp. 23-40.

Emmanuel, Esther. “Data Protection Challenges in Developing Countries: A Nigerian Perspective.” Africa Data Law Journal, vol. 4, no. 2, 2023, pp. 54-72.

Garcia, Laura. “Smart Cities and the Role of IoT in Urban Planning.” Urban Tech Journal, vol. 15, no. 4, 2023, pp. 112-130.

Gellman, Robert, and Paul Schwartz. “Data Protection Law and Compliance.” Oxford University Press, 2018.

Greenleaf, Graham. “Global Data Privacy Laws 2018: 120 National Laws and Many More to Come.” Privacy Laws & Business International Report, vol. 156, 2018, pp. 10-13.

Johnson, Kevin. “Data Aggregation Risks in IoT: The Privacy Implications of AI.” Cybersecurity Review, vol. 9, no. 2, 2023, pp. 87-103.

Karim, Faiza. “Cybersecurity Challenges in Large IoT Networks.” Global Cybersecurity, vol. 19, no. 2, 2024, pp. 34-51.

Kshetri, Nir. “The Economics of the Internet of Things.” IEEE IT Professional, vol. 19, no. 5, 2017, pp. 32-39.

Lee, Jason. “Data Minimization Principles in AI-IoT Systems.” Journal of Data Ethics, vol. 14, no. 2, 2023, pp. 45-65.

Miller, George. "Re-identification in Anonymized Data: Risks of AI in IoT Systems." PrivacyTech Journal, vol. 7, no. 1, 2023, pp. 98-115.

Nwogu, Chidinma. “The Nigeria Data Protection Act and Global Data Privacy.” PrivacyLaw Press, 2023.

Nwosu, Ugochi. “Strong Cybersecurity Measures in IoT: A Nigerian Case Study.” Africa Technology Review, vol. 8, no. 4, 2023, pp. 23-39.

O'Connell, David. “Bias and AI: Ethical Concerns in Predictive Systems.” AI Ethics Journal, vol. 5, no. 2, 2023, pp. 65-89.

Patel, Ramesh. “General Data Protection Regulation (GDPR) and Its Global Influence.” International Data Privacy Review, vol. 10, no. 1, 2023, pp. 101-115.

Park, Jihoon. “International Agreements on IoT Security Standards.” Journal of Global Cybersecurity, vol. 5, no. 1, 2024, pp. 16-29.

Patel, Ramesh. “General Data Protection Regulation (GDPR) and Its Global Influence.” International Data Privacy Review, vol. 10, no. 1, 2023, pp. 101-115.

Roberts, James. “AI’s Impact on Re-identifying Data: A Privacy Threat in IoT.” Journal of Data Science and Privacy, vol. 12, no. 1, 2024, pp. 80-97.

Silva, Maria. “Algorithmic Transparency in AI: Legal and Ethical Considerations.” International Journal of AI Law, vol. 9, no. 1, 2023, pp. 11-29.

Smith, John. “AI and IoT: Convergence in the Digital World.” TechPress, 2022.

Solove, Daniel J. “Understanding Privacy.” Harvard University Press, 2008.

Summayah Muncey. “AI and data privacy in big-tech: A new frontier in the digital market.” Journal of Data Protection & Privacy, vol. 6, 3 256–265.

Taylor, Alicia. “Informed Consent in IoT Devices: A Legal Analysis.” Tech Law Review, vol. 14, no. 3, 2022, pp. 76-93.

Tufekci, Zeynep. “Twitter and Tear Gas: The Power and Fragility of Networked Protest.” Yale University Press, 2017.

Tunde, Ayo. “Ownership of Data in AI-IoT Systems: A Legal Perspective.” Nigeria Law Journal, vol. 11, no. 3, 2024, pp. 53-77.

Williams, Rebecca. “The Intersection of Competition Law and Data Protection in AI Ecosystems.” Global AI Law Journal, vol. 9, no. 4, 2023, pp. 76-89.

Williams, Sarah. “Ethics in AI: Challenges in IoT Ecosystems.” EthicsTech Publishing, 2024.

Zhao, Li. “Balancing Innovation and Privacy in AI-IoT Ecosystems.” Global Technology Review, vol. 22, no. 3, 2023, pp. 94-110.

Zuboff, Shoshana. “The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.” Public Affairs, 2019.

Rethinking Consent-Based Data Protection and Privacy in Nigeria: Toward a Harm-Accountability Framework

David Odes
Web Security Lab

Abstract

This paper critically examines the limitations of Nigeria's consent-based data protection framework under the *Nigeria Data Protection Act 2023* (NDP Act or the Act) and proposes a transition to a harm-accountability model. The consent-based approach, rooted in rational choice theory, assumes that individuals provide informed and rational consent for their data to be processed. However, behavioural economics and empirical research challenge this assumption, citing cognitive biases, informational asymmetry, and the complexities of digital decision-making. These flaws undermine consent as an effective mechanism for privacy protection. Using a mixed-methods approach—integrating legal critique, theoretical exploration, and stakeholder surveys—this paper highlights the inadequacies of the current framework. It proposes a harm-accountability model, emphasising data controllers' accountability through compliance and proactive risk management, and strict penalties for breaches, regardless of user consent. This model addresses the challenges of Nigeria's growing digital economy. To operationalise this framework, the paper recommends legislative reforms and policy measures to strengthen accountability and enhance data subject protection.

Keywords: Consent-Based Framework, Harm-Accountability, Data Protection, Privacy, Nigeria.

1. Introduction

The exponential growth of digital technology has transformed how personal data is collected, processed, and shared. In developing economies such as Nigeria, data privacy laws often rely on consent-based frameworks to safeguard individuals' digital rights. The NDP Act mandates consent in specific high-risk scenarios, such as the processing of sensitive data, direct marketing, or cross-border data transfers, to ensure user control. However, the consent-based model assumes that individuals can fully understand and rationally evaluate the implications of their decisions. Rooted in contract law, it treats privacy as a transaction where individuals freely accept or reject terms.

In practice, users encounter complex privacy agreements, manipulative "dark pattern" interfaces, and "take-it-or-leave-it" consent options that undermine meaningful control. Furthermore, the ubiquity of digital services makes refusing consent impractical, often excluding users from essential online functions. Behavioural economics further exposes flaws in this model, demonstrating how cognitive biases, incomplete information, and environmental pressures impair decision-making.

A recent survey of 200 Nigerian internet users revealed significant gaps in understanding and engagement with consent mechanisms. Despite expressing privacy concerns, users frequently remain unaware of or unable to comprehend the terms they accept. This paper advocates for a harm-accountability model to complement consent in situations where it is required. By shifting the focus from procedural compliance—where obtaining consent is treated as an end in itself—to outcome-based accountability, this model

emphasises proactive risk mitigation by data controllers, ensuring stronger safeguards against privacy harms.

2 Literature Review

This review examines the theoretical underpinnings of consent-based data protection frameworks and their critiques, focusing on rational choice theory, behavioural economics, regulatory responses, and the localised challenges in Nigeria.

2.1 Rational Choice Theory

The concept of informed consent in data protection stems from liberal philosophical traditions emphasising individual autonomy and rational decision-making (Solove 1895). This framework assumes individuals can make optimal choices about their privacy when provided with adequate information. This model treats privacy as a commodity that individuals can freely trade through informed consent decisions. This has shaped global data protection frameworks, including Nigeria's NDP Act, which emphasises transparent information disclosure and user consent as primary protective mechanisms.

2.2 Behavioural Economics Critique

Behavioural economics challenges the assumptions of rational choice theory by highlighting the cognitive biases that shape decision-making. Simon's foundational theory of bounded rationality fundamentally challenges these assumptions by demonstrating how cognitive limitations prevent individuals from making utility-maximising decisions (Simon 103-104). When applied to privacy decision-making, behavioural economists like Acquisti and Grossklags argue that users are often unable to make fully in-

formed and optimal privacy choices due to cognitive overload and biases (Acquisti and Grossklags 26-27, 31-32).

Recent studies have further documented how certain design practices—often referred to as "dark patterns"—manipulate users into making privacy-invasive decisions (Utz et al. 973; Nouwens et al. 1, 3). These findings are particularly relevant in developing economies like Nigeria, where digital literacy levels vary significantly. In such contexts, users may be more susceptible to manipulation through confusing or misleading consent mechanisms. Studies have identified several behavioural limitations in privacy decision-making, including:

- Information asymmetry between users and data controllers
- Cognitive overload from complex privacy decisions
- Status quo bias leading to acceptance of default settings
- Cultural prioritisation of immediate benefits over long-term risks, often influenced by trust heuristics
- Present bias in evaluating privacy risks

2.3 Localised Challenges in Nigeria

While existing literature extensively documents the limitations of consent-based frameworks in Western contexts, significant gaps remain in understanding how these frameworks operate in developing countries like Nigeria. In Nigeria, rapid digital adoption coincides with unique cultural perspectives on privacy, behavioural tendencies, and varying levels of digital literacy. These factors challenge the effectiveness of consent-based models that assume informed and rational decision-making by users. Yisa et al. (2023) highlight that Nigerians prioritise immediate benefits, such as financial rewards or improved service quality, over long-term risks like data misuse. Their study demonstrates that **perceived benefits**, rather than **perceived sensitivity** (risks), play a dominant

role in users' privacy decision-making (Yisa et al. 294). Gender differences were also observed, with women showing greater caution and reliance on trust in platforms to mitigate perceived risks. Trust heuristics, such as confidence in a platform's reputation or design, frequently replace critical evaluation of consent forms (Yisa et al. 295). These findings highlight the inadequacy of consent-based models in Nigeria, where cognitive biases and limited digital literacy dominate decision-making. This study builds on these insights to propose a **harm-accountability framework** that shifts the burden of privacy protection from users to organisations, ensuring robust safeguards tailored to Nigeria's digital landscape.

2.4 Regulatory Responses and Emerging Solutions

Scholars and policymakers have proposed regulatory frameworks that move beyond the consent-based model. Solove, for example, advocates for data protection systems that prioritise transparency and corporate accountability rather than relying solely on individual consent. This shift is reflected in modern regulations like the European Union's General Data Protection Regulation (European Union), which supplements consent with measures such as privacy by design and data minimisation, and theCalifornia Consumer Privacy Act (California State Legislature), which introduces corporate accountability through opt-out mechanisms and user rights.

While these frameworks represent progress, they remain rooted in procedural compliance and user choice, falling short of the harm-accountability approach. Nigeria's NDP Act similarly retains a consent-based model, incorporating similar provisions but lacking proactive measures to address cognitive and behavioural challenges or ensure accountability for harmful outcomes. True data protection requires a model that which holds organisations accountable for outcomes, even when they adhere to lawful bases for processing as this evolution is crucial to address the realities

of digital ecosystems where user understanding and agency are often constrained.

3 Methodology

This study employed a mixed-methods approach to examine the limitations of consent-based data protection frameworks in Nigeria and evaluate the potential for a harm-accountability model. The research design incorporated both quantitative and qualitative elements to provide comprehensive insights into privacy decision-making behaviours and attitudes.

3.1 Research Design

The mixed-methods approach integrated quantitative data to identify statistical patterns with qualitative feedback to uncover deeper motivations and challenges. This ensured a holistic understanding of the limitations of consent-based frameworks in Nigeria.

3.2 Data Collection

3.2.1 Survey Instrument

The primary instrument was an online survey conducted between 5 and 25 November 2024, designed using behavioural economics principles to explore present bias and information asymmetry in privacy decisions.

3.2.2 Sampling Method

Participants were recruited through a self-selecting sampling method via social media platforms. While participants could choose their age group from predefined categories, the sampling did not

involve random selection, which may result in biases. A total of 200 Nigerian internet users participated in the survey.

3.2.3 Survey Content

The survey included both structured and open-ended questions, covering the following areas:

- Internet usage patterns and device preferences.
- Engagement with privacy consent mechanisms.
- Comprehension of privacy terms.
- Attitudes toward corporate accountability.
- Preferences for privacy control mechanisms

3.3 Data Analysis

Quantitative responses were analysed using descriptive statistics to identify behavioural patterns, while qualitative feedback underwent thematic analysis to explore nuanced perspectives. This dual approach provided both broad trends and context-specific insights into user behaviour and attitudes.

3.4 Ethical Considerations

The study adhered to ethical research practices. Participants provided informed consent, and confidentiality was maintained throughout. No personally identifiable information was collected, and participants retained the right to withdraw at any time.

3.5 Study Limitations

The study acknowledges the following limitations:

- Sampling Bias: The self-selecting sampling method may overrepresent younger, tech-savvy individuals, particularly in the 18–25 age group.
- Urban Bias: Responses likely reflect urban users, limiting generalisability to rural populations.
- Self-Reporting Bias: Results depend on participants' subjective interpretations of survey questions.

4 Results and Discussion

This section presents the findings from the survey of 200 Nigerian internet users, providing insights into the challenges and limitations of the consent-based data protection framework.

4.1 Age Demographics and Internet Usage Patterns

The demographic breakdown revealed that 75% of respondents were in the 18–25 age group, with smaller percentages in older age groups. This demographic is highly relevant as younger users tend to be more active online and are often targeted by tech companies for data collection. The high rate of daily internet use (95%) and prevalence of smartphone usage (92%) highlight the importance of optimising privacy mechanisms for mobile-first users. Many consent prompts, including cookie pop-ups and terms of service agreements, are designed with desktop users in mind. This finding suggests a need to optimise consent mechanisms for mobile devices, where users may face additional challenges in understanding the implications of their consent, due to smaller screens and more complex layouts.

4.2 Reading and Understanding Consent Prompts

The results reveal that 54% of users either rarely or never read consent prompts, and another 37% read them only sometimes.

These findings suggest a clear disengagement with consent requests. While this behaviour may be partly due to the overuse of consent prompts on many websites, it also highlights a deeper issue: users are likely overwhelmed by the sheer volume of information presented to them. This aligns with cognitive load theory, which posits that excess information overwhelms decision-making, leading users to default acceptance.

4.3 Understanding and Feeling Informed About Consent

Only 17% of respondents claim to fully understand the information provided in consent prompts, while 48% somewhat understand, and 20% find the information confusing. This is a key insight, indicating that even when users engage with consent prompts, many do so with limited comprehension. The language used in consent prompts is often technical, legalistic, and dense, which can alienate users, especially those without formal education in legal or technical matters. This issue is particularly acute in Nigeria, where digital literacy remains a challenge, even in urban areas. Moreover, 36% of respondents feel unsure when accepting consent, and 20% never feel fully informed. This highlights a significant gap between the ideal of informed consent and the reality of data privacy practices. Informed consent, as envisaged in the NDP Act, presupposes that individuals have the capacity to make autonomous decisions based on full knowledge of the consequences. However, the survey findings reveal that many Nigerians lack this capacity due to the inherent flaws in the design and presentation of consent prompts.

4.4 Declining Consent and Control Over Data

When asked whether they have ever declined consent on a website or app, 94% of respondents either frequently or rarely declined consent. Despite this, the 6% who "usually just accept" de-

monstrates the default nature of consent acceptance. Many users, even when aware of the option to decline, choose to accept terms for convenience or due to a lack of understanding of what rejection entails. The concept of consent fatigue is prevalent, especially when faced with multiple prompts across different platforms. Furthermore, when given the option to control specific permissions (e.g., choosing what data to share), 71% of respondents indicated they would definitely use such options. This strong preference for control over data use suggests that Nigerians want more granular, transparent privacy settings, where they can actively choose how their data is used. The desire for user-centric data control challenges the assumption that blanket consent is sufficient to protect individuals' privacy.

4.5 Concerns About Data Privacy and Accountability

Privacy concerns are highly prevalent in the survey, with 69% of respondents expressing being very concerned about the privacy of their personal data online. This finding aligns with broader global trends, where data breaches and the misuse of personal data have become major issues. Nigerians, particularly young internet users, are acutely aware of the risks of data misuse, especially in the context of rampant cybercrime and identity theft. More importantly, the survey reveals strong support for a shift in the responsibility for data protection. 57% of respondents strongly agree that companies should be held accountable for privacy harms, even if the user has given consent. This finding is significant, as it signals a preference for a harm-accountability model in data protection that goes beyond user consent to hold companies responsible for any misuse of personal data. In addition, 71% of respondents agree that data protection should extend beyond consent to hold companies accountable for misuse. This aligns with the growing trend in data protection laws that recognise the limitations of consent and call for a more comprehensive approach to safeguarding users' data.

5 Recommendations

The findings reveal that the current consent-based framework under the NDP Act is inadequate for ensuring meaningful data protection. To address this, the paper proposes transitioning to a harm-accountability framework, which complements user consent with stronger corporate responsibility. The recommendations focus on addressing the cognitive limitations of users and improving accountability mechanisms.

5.1 The Case for a Harm-Accountability Framework in Nigeria

The survey findings highlight the critical need for a harm-accountability framework. With 83% of respondents reporting limited or no understanding of consent prompts and a predominantly young, mobile-first internet user base, the current model is ineffective. Key recommendations for the harm-accountability approach include:

Addressing Inadequate Understanding:

- Shift the focus from user consent to corporate responsibility for minimising risks.
- Mandate privacy by design principles and proactive data protection measures, irrespective of consent status.
- Bridge comprehension gaps through simplified and transparent consent mechanisms.

Optimising for Mobile Interfaces:

- Replace overly complex consent interfaces with user-friendly designs optimised for mobile devices.

- Require privacy-protective defaults tailored to mobile-first users and varying levels of digital literacy.

Strengthening Corporate Accountability:

- Hold companies legally accountable for privacy harms, even when consent has been obtained.
- Require proactive risk assessments and a duty-of-care approach akin to GDPR and CCPA standards.
- Enforce strict penalties for data breaches and misuse.

Empowering Users Through Alternatives:

- Implement granular data control mechanisms to allow users to specify how their data is used.
- Mandate transparency in data-handling processes and provide clear reporting on protection measures.

5.2 Implementation Framework

Transitioning to a harm-accountability model requires legislative, organisational, and infrastructural reforms.

5.2.1 Legal Framework Adaptation

To facilitate a meaningful transition to a harm-accountability framework, the NDP Act must be amended to incorporate principles that prioritise proactive harm prevention and corporate accountability. While Sections 24–28 of the Act establish foundational principles such as lawfulness, transparency, and purpose limitation, they primarily emphasise procedural safeguards rather than the prevention of privacy harms that may arise even when

processing adheres to lawful bases. The harm-accountability framework shifts the focus from compliance to outcomes, emphasising the following:

- **Proactive Harm Prevention**: Mandating that data controllers identify and mitigate a wide range of potential harms—such as identity theft, financial exploitation, reputational damage, emotional distress, or other adverse outcomes—regardless of consent.
- **Outcome-Based Accountability**: Extending liability to data controllers for harms caused by their activities, even if they comply with lawful bases under Section 25 of the NDP Act.

These principles provide the foundation for a harm-accountability approach, which can be operationalised through specific amendments to the NDPAct:

- Define Privacy Harms: Establish clear categories of harm, such as financial loss, reputational damage, emotional distress, or other adverse impacts on individuals, to provide standards for enforcement and accountability.
- Mandate Harm Mitigation Plans: Require data controllers to include harm mitigation strategies in compliance audits, ensuring proactive risk management.
- Expand DPIA Requirements: Mandate Data Privacy Impact Assessments (DPIAs) for all processing activities, incorporating ongoing risk assessments to adapt to evolving threats.
- Introduce Penalties for Failure to Prevent Harm: Establish penalties for data controllers who fail to prevent harm, even when processing adheres to lawful bases.
- Strengthen Redress Mechanisms: Enhance mechanisms to ensure accessible and effective remedies for data subjects harmed by processing.

5.2.2 Capacity Building for Regulators

Building the necessary capacity for the new framework will require targeted training and development initiatives. Regulatory staff must be trained in harm-assessment methodologies, and technical capacity within the Nigeria Data Protection Commission (NDPC) must be significantly enhanced. Programs aimed at improving business understanding of privacy-protective practices should be implemented, alongside initiatives to boost digital literacy among users. Furthermore, establishing mechanisms for regular privacy audits and compliance monitoring will be crucial to maintaining the integrity of the system. The NDPC should also introduce penalties for organisations that deploy manipulative design practices, such as "dark patterns," or fail to provide meaningful privacy controls. Specific guidelines should define and prohibit deceptive practices, requiring organisations to implement user-friendly, transparent consent mechanisms. Financial penalties and public disclosure of corrective actions should be imposed on violators, while privacy-by-design practices should be incentivised to promote compliance and accountability.

5.2.3 Business Impact and Support

For businesses, the transition to a harm-accountability model will require significant structural adjustments. Organisations will need to develop new risk assessment protocols, implement stronger data protection measures, and create more transparent data-handling processes. Investments in privacy-enhancing technologies will be essential, as will ongoing training for staff on privacy-protective practices.

6 Conclusion

This paper has examined the limitations of consent-based data protection frameworks in Nigeria and proposed a shift toward a

harm-accountability model. A survey of 200 Nigerian internet users revealed significant challenges, including consent fatigue, cognitive barriers, and limited understanding of consent prompts. The current framework fails to provide robust privacy protection for most Nigerians and the findings in this paper highlight strong public support for better corporate accountability, with 57% of respondents favouring liability for privacy harms regardless of consent and 71% desiring greater control over personal data.

Future research should explore implementation challenges, including harm assessment criteria, impacts on SMEs, regulatory integration, cross-border data flows, and enforcement mechanisms. As Nigeria's digital economy grows, adopting a harm-accountability framework is essential to ensure robust privacy protection, foster user trust, and promote responsible corporate data practices. This transition will require collective effort from policymakers, businesses, and civil society, but its potential benefits—enhanced privacy and protection, greater trust, and improved accountability—make it a necessary evolution for Nigeria's digital future.

Works Cited

Acquisti, Alessandro, and Jens Grossklags. "Privacy and Rationality in Individual Decision Making." IEEE Security & Privacy, Vol. 3, no. 1, 2005, pp. 26-33.

European Union. "General Data Protection Regulation." EUR-Lex, 27 Apr. 2016, eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

California State Legislature. "California Consumer Privacy Act." California Legislative Information, 2018, oag.ca.gov/privacy/ccpa.

Federal Republic of Nigeria. "Nigeria Data Protection Act." Nigerian Government, 2023, cert.gov.ng/ngcert/resources/Nigeria_Data_Protection_Act_2023.pdf.

Simon, Herbert A. "A Behavioral Model of Rational Choice." The Quarterly Journal of Economics, Vol. 69, no. 1, 1955, pp. 99-118.

Solove, Daniel J. "Privacy Self-Management and the Consent Dilemma." Harvard

Law Review, Vol. 126, no. 7, 2013, pp. 1880-1903.

Nouwens, Midas, et al. "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence." Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, Association for Computing Machinery, 2020, pp. 1-12.

Utz, Christine, et al. “(Un)informed Consent: Studying GDPR Consent Notices in the Field.” 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS ’19), ACM, 2019, pp. 973–989.

Yisa, Victor L., et al. "Investigating Privacy Decision-Making Processes Among Nigerian Men and Women." Proceedings on Privacy Enhancing Technologies, Vol. 2023, no. 1, 2023, pp. 294–308.

Appendix A: Survey Questions

Basic Information

1. **Age Group**
   a) Under 18
   b) 18-25
   c) 26-35
   d) 36-50
   e) Over 50

2. **How often do you use the internet?**
   a) Daily
   b) Several times a week
   c) Weekly
   d) Rarely

3. **What type of device do you mostly use to browse the internet?**
   a) Smartphone
   b) Tablet
   c) Computer
   d) Other

Consent Prompts and Understanding

4. **When you see a consent prompt (like cookie pop-ups or terms of service agreements), do you read it before accepting?**
   a) Always
   b) Sometimes
   c) Rarely
   d) Never

5. **How well do you understand the information provided in consent prompts?**
   a) I fully understand them
   b) I somewhat understand them
   c) I find them confusing
   d) I don't understand them at all

6. **Do you feel that you have enough information to make an informed decision when accepting a consent prompt?**
   a) Yes, definitely
   b) Sometimes
   c) No, I often feel unsure
   d) I never feel fully informed

7. **Have you ever declined consent on a website or app?**
   a) Yes, frequently
   b) Yes, but rarely
   c) No, I usually just accept

8. **If you were given more control over data use (e.g., choosing specific permissions), would you likely use it?**
   a) Definitely
   b) Maybe
   c) Probably not

Privacy Concerns and Accountability

9. **How concerned are you about the privacy of your personal data online?**
   a) Very concerned
   b) Somewhat concerned
   c) Neutral
   d) Not concerned

10. **Would you feel more protected if companies were held accountable for privacy harms, even if you had given consent?**
    a) Strongly Agree
    b) Agree
    c) Neutral
    d) Disagree
    e) Strongly Disagree

11. **Do you think data protection should go beyond consent to hold companies responsible for any misuse of your data?**
    a) Yes, absolutely
    b) Maybe, depending on the situation
    c) No, I think consent is enough

Open-Ended Questions

12. **In your experience, what challenges do you face when trying to understand privacy terms on websites or apps?**

13. **What changes would make you feel more in control of your data privacy online?**

This survey was conducted in English and distributed through online channels targeting Nigerian internet users between November 2024. The survey was optimised for both mobile and desktop completion.

Redefining Global Data Governance: The Case for Data Embassies

Fernandez Marcus-Obiene, LLM (LegalTech)
Special Assistant to the Nigerian President on Justice Sector Reform and ICT/Digital and Innovative Technology

Abstract:

This paper examines the concept of data embassies as a revolutionary solution to the challenges of cross-border data governance in an increasingly digitalized world. Drawing parallels with traditional diplomatic missions, data embassies represent secure, extraterritorial data centers that operate under the jurisdiction of their home countries while being physically located abroad. Estonia's pioneering implementation of a data embassy in Luxembourg serves as a case study, demonstrating how this framework can effectively address the fundamental tension between national sovereignty and global connectivity in data management while facilitating secure cross-border data flows.

The study proposes the development of a comprehensive international treaty to address critical challenges facing the widespread adoption of data embassies, including concerns over national sovereignty, variations in privacy standards, and the need for robust international oversight. This treaty would establish global privacy standards, mandate independent audits, and create accountability mechanisms for data breaches. While data embassies represent a transformative approach that could revolutionize how countries manage and protect digital assets, their successful implementa-

tion depends on significant international cooperation and standardized protocols for data protection and security.

Keywords: Data governance; Data embassies; Cross-border data transfers; Privacy; National security

1. Introduction: The Dilemma of Data Sovereignty and Governance

In today's digital age, data is the lifeblood of global economies. Every industry, from finance and healthcare to entertainment and technology, relies heavily on the smooth and secure transfer of information across borders. However, as crucial as data is, the legal frameworks that govern its flow are fragmented and often conflicting, making cross-border data transfers a legal minefield.

At the heart of this dilemma is the tension between national sovereignty and the need for global connectivity. Governments are naturally concerned about who controls sensitive data, how it's used, and how their citizens' privacy is protected. These concerns lead to strict regulations that make it harder for businesses to operate across borders. The problem becomes even more pronounced when national security is at stake ((Kharazishvili & Kwiliński, 2023). The result? An intricate web of laws and regulations that often slows down or restricts the flow of data (Greenleaf, 2014).

2. A Complex Web of National and International Regulations

Efforts to regulate cross-border data transfers vary significantly from one region to another. In the European Union, the GDPR sets

one of the strictest frameworks for data protection, placing heavy restrictions on data transfers to countries outside the EEA. Nigeria has a similar framework as the EU. The United States, on the other hand, adopts a more fragmented approach, with sector-specific regulations that govern areas like healthcare and financial services (Schwartz, 2019).

Attempts to harmonise these conflicting regulatory frameworks—such as the EU-U.S. Privacy Shield—have struggled. The Privacy Shield's invalidation in 2020 was a stark reminder of how difficult it is to bridge these legal gaps (Court of Justice of the European Union - Case C-311/18). Multinational companies find themselves navigating a maze of requirements, each new country posing a new set of legal hurdles. This is where the concept of data embassies comes in—an idea that has the potential to transcend these jurisdictional boundaries.

3. Historical Context

The concept of data embassies emerged in the backdrop of increasing cyber threats and the evolving landscape of data sovereignty. It was prominently initiated by Estonia, which established the first data embassy in Luxembourg in response to significant cyberattacks in 2007. These attacks were triggered by political unrest following Estonia's decision to relocate a Soviet-era war memorial, highlighting the nation's vulnerability to digital threats that could disrupt essential governance functions and services reliant on digital infrastructure (Shrivastava and Lakra, 2024).

The concept of data embassies represents a transformative approach to addressing the legal complexities of cross-border data governance. By borrowing from the principles that govern diplomatic missions—where embassies are considered the sovereign territory of the sending nation regardless of their physical location in a foreign country—data embassies create a framework

where data centers are legally extraterritorial. This allows them to operate under the laws of their home country rather than being subject to the jurisdiction and laws of the host nation where they are physically located.

Data embassies serve as secure locations for storing critical governmental data outside a nation's borders, operating under diplomatic immunity akin to traditional embassies. This framework allows countries to safeguard their digital assets from potential risks, such as cyberattacks and natural disasters, while ensuring continuity of governance even in the face of infrastructural failures. The Estonian model set a precedent, leading other nations, such as Monaco, to follow suit in establishing their own data embassies for similar protective reasons.

This approach offers several advantages. First and foremost, it provides a legal "safe zone" for data storage and processing, ensuring that sensitive data is protected from local government interference or legal demands that may compromise its security or the privacy rights of individuals. The legal discourse around data embassies has highlighted the necessity for a robust framework that aligns with international norms while addressing domestic requirements. Legal experts have noted the complexities surrounding jurisdictional issues and the need for clarity in operational laws governing these entities. Discussions are ongoing to establish comprehensive guidelines to enhance legal protections for both local and foreign stakeholders involved in data handling (India Press Agency, 2024).

Estonia's pioneering efforts in this domain provide a concrete example of how this concept could work in practice. In 2017, Estonia became the first country to establish a data embassy in Luxembourg, storing its critical state data in a secure data center that operates under Estonian jurisdiction, despite being physically located in another country (Shrivastava and Lakra, 2024). This ensures that Estonia's critical digital assets, including government

data and essential services, are protected from external threats while remaining under Estonian legal control.

The global expansion of data embassies could help address the inconsistencies in national data protection laws. Currently, companies and governments operating across borders face a patchwork of regulations that can be challenging to navigate, particularly when it comes to data storage and processing. The rules governing data protection in the European Union (EU), for instance, are among the most stringent in the world under the General Data Protection Regulation (GDPR), while other countries have more lenient or sector-specific laws.

The concept of data embassies not only represents a novel approach to data governance but also signifies a shift in how nations perceive and manage their data sovereignty in an interconnected digital world (Sarkar and Sarkar, 2023). As countries increasingly recognize the importance of secure data management, initiatives to create data embassies are expected to grow, facilitating a global shift toward enhanced digital security and cooperation among nations (Meyer, 2022).

4. Case Studies and Examples

4.1 Estonian Data Embassy

The Estonian data embassy, established in Luxembourg, serves as a pioneering example of how nations can secure their digital continuity. In 2016, Estonia and Luxembourg signed a Memorandum of Understanding to host critical data and information systems outside Estonia's physical borders, with the formal agreement ratified by both parliaments in 2018 (Shrivastava and Lakra, 2024). This data embassy operates as a backup for essential datasets, including the e-file court system, treasury information, and population registers. It is designed to ensure the continuity of government

functions in the face of threats such as natural disasters, cyberattacks, or military invasions, allowing Estonia to maintain operational capabilities even if governing from within its own territory is compromised.

4.2 Monaco's Data Embassy

Following Estonia's lead, Monaco has also established a data embassy in Luxembourg. This initiative reflects the growing recognition of the importance of safeguarding critical government data in secure, foreign locations (Basu, 2023). Like the Estonian model, Monaco's data embassy aims to provide a high level of security and act as a vital backup for governmental data, ensuring continuity during crises.

4.3 India's Proposed Data Embassies

In February 2023, the Government of India announced plans to allow the establishment of data embassies within its territory. This initiative aims to attract international investment in digital infrastructure by offering countries and corporations the opportunity to build data centers in designated Special Economic Zones. The proposed data embassies would enjoy diplomatic immunity from local laws, thus creating secure environments for sensitive data management (Basu, 2023). This move indicates a shift towards adopting the data embassy concept more broadly, promoting digital security and continuity for various nations and organizations.

5. The Benefits of Data Embassies: Beyond Legal Immunity

At first glance, data embassies may appear to be a convenient way to bypass national regulations, but their potential impact goes far

beyond simply offering immunity from local laws. The true strength of data embassies lies in their ability to build trust and transparency in a globalized digital economy, where cross-border data flows are increasingly vital. With data embassies, businesses, governments, and individuals can store and process their data in a secure environment, free from concerns about undue government surveillance, overreach, or arbitrary legal demands from foreign authorities (Samanta, 2024).

This trust-based framework addresses some of the most pressing challenges in the digital age, particularly the lack of confidence many entities have when transferring data across borders. For instance, multinational corporations often face regulatory bottlenecks when dealing with differing national laws that complicate the storage and movement of data between countries. By allowing data embassies to operate under the jurisdiction of their home countries, businesses would no longer need to navigate the complexities of a patchwork of conflicting data regulations, as the data stored in these embassies would be governed by a single legal regime. This could significantly streamline data management processes, boosting efficiency and facilitating global commerce.

Data embassies also offer the potential to standardize data protection laws internationally. Currently, one of the biggest challenges to cross-border data flows is the variance in data protection standards across different jurisdictions (Samanta, 2024). For example, while the European Union's General Data Protection Regulation (GDPR) imposes some of the world's strictest privacy standards, other countries have more lenient regulations, particularly when it comes to government access to data for law enforcement or national security purposes. Data embassies could help harmonize these standards by establishing a global framework for data protection, wherein participating countries agree to a unified set of rules and best practices, thus reducing the legal friction between nations.

By facilitating international collaboration on data governance, the data embassy framework would encourage countries to adhere to internationally recognized privacy and security protocols, such as the ISO/IEC 27001 standard for information security management. These standards, audited by independent bodies, would ensure that data embassies maintain the highest levels of cybersecurity. Regular independent audits would add an extra layer of accountability, reassuring both governments and businesses that data stored in embassies is not only protected from legal threats but also from cybersecurity breaches.

Moreover, the idea of data embassies fosters the possibility of creating a global data infrastructure that is both secure and resilient. For instance, a network of data embassies could provide backup for critical data in cases of national crises, cyberattacks, or natural disasters, ensuring the continuity of essential services and minimizing the risk of data loss. Governments could store copies of their most important digital assets in data embassies located in allied countries, much like Estonia's decision to store its critical state data in Luxembourg.

In this way, data embassies could not only boost cybersecurity but also ensure the resilience of global digital infrastructure, providing a trusted and secure solution for data storage in an increasingly interconnected world. As the digital economy continues to expand, the establishment of data embassies could become a cornerstone of international data governance, promoting trust, transparency, and collaboration in a manner that transcends national boundaries.

6. Overcoming the Obstacles: Addressing Criticisms and Concerns

The idea of data embassies is not without significant challenges, the foremost of which is the concern over national sovereignty.

Governments may be reluctant to relinquish control over data stored within their borders, especially when it comes to sensitive information or matters involving national security (Tonomus Neom, 2024). The idea of allowing data to exist beyond the legal reach of the host country, even while physically present on its soil, may provoke strong resistance from some nations. This reluctance stems from the fear that data embassies could be used to shield information from local law enforcement or to conceal activities that could pose a threat to national security.

To mitigate these concerns, the framework for data embassies would need to include clear and transparent guidelines on when and how governments can access data. An independent international oversight body could play a key role in regulating such access, ensuring that data is only retrieved for legitimate, narrowly defined purposes, such as investigations into terrorism, international crime, or imminent national threats (Culver. 2020). By requiring government requests for data to pass through a standardized process, overseen by a neutral body, the framework would provide a balanced approach that protects both national security and individual privacy rights.

In addition to oversight, an international arbitration system could be established to handle disputes, particularly in cases of data breaches or disagreements over the scope of government access. This arbitration system would ensure that accountability is maintained on a global scale, and that data embassies operate with a level of legal clarity that benefits all participating nations. The system could also address potential conflicts between host countries and the home nations of data embassies, preventing legal and political disputes from stalling the flow of information.

Another major challenge involves the variation in privacy standards across different countries. What constitutes adequate protection of personal data in one nation might fall short in another, especially when comparing countries with stricter privacy regulations—like those in the European Union under the General Data

Protection Regulation (GDPR)—to those with more lenient or sectoral privacy frameworks, such as the United States. This inconsistency makes it difficult to create a global system that satisfies all parties involved.

One possible solution is to introduce a minimum global privacy standard, ensuring that all data embassies operate under a consistent set of rules. This would establish a baseline level of data protection that aligns with widely recognized frameworks, such as the GDPR or ISO/IEC 27001 for information security. By adhering to these internationally recognized standards, data embassies would offer a level of privacy and security that reassures individuals, businesses, and governments alike that their data is adequately protected.

For countries with stricter privacy laws, the treaty could allow for the application of higher privacy standards within specific embassies. This would create a system of "privacy tiers," where data embassies in more privacy-conscious jurisdictions—such as within the European Union—could offer enhanced protections. This flexible system would help bridge the gap between nations with varying approaches to data privacy, while still maintaining a cohesive global framework for data governance.

In this way, the concept of data embassies could strike a delicate balance between the competing interests of national sovereignty, global commerce, and individual privacy. By building trust through transparency, independent oversight, and international cooperation, data embassies could provide a secure, adaptable solution to the challenges of cross-border data governance in the digital age.

7. Toward a Global Treaty on Data Embassies

To implement the data embassy model on a global scale, an international treaty would be essential. This treaty would need to ad-

dress a range of critical issues, from legal jurisdiction to data protection standards, ensuring that data embassies operate within a clearly defined global framework. By establishing a comprehensive set of rights and responsibilities, such a treaty would create a standardized system for privacy, security, and oversight, making data embassies viable in different jurisdictions while fostering global trust in the system.

The key elements of such a treaty would likely include:

1. Global Privacy Standards: A cornerstone of the treaty would be the creation of a global baseline for privacy protection, aligned with well-established frameworks such as the GDPR. This would ensure that individuals' data is safeguarded consistently, regardless of where it is stored. While the baseline would set minimum protections, the treaty would allow for stricter national interpretations, giving countries the flexibility to impose higher standards of privacy protection if they deem it necessary. This balance between global consistency and national autonomy would help address concerns about privacy sovereignty.
2. Independent Audits: To ensure that data embassies maintain high levels of security and adhere to the agreed-upon privacy standards, the treaty would mandate regular independent audits. These audits, conducted by neutral international bodies, would assess the embassies' compliance with privacy, security, and transparency requirements. Publicly accessible audit results would further enhance trust, ensuring that data embassies are held accountable for maintaining the necessary protections. Transparency reports, similar to those issued by large tech companies today, could be required to disclose government access requests or security incidents, adding another layer of oversight.
3. Conditional Government Access: One of the most contentious issues in cross-border data management is government access

to private data, particularly in cases involving national security or law enforcement. The treaty would need to create transparent rules outlining the conditions under which governments could access data stored in embassies. These conditions would include narrowly defined circumstances, such as terrorism investigations or imminent threats to national security, and would require proper judicial oversight. Moreover, the treaty could provide for international arbitration to resolve disputes over access requests, ensuring that no government abuses its powers by circumventing privacy protections. The inclusion of an impartial dispute resolution mechanism would prevent conflicts between nations and protect the integrity of the system.

4. Accountability Mechanisms: Given the sensitive nature of the data stored in embassies, a clear and robust system for addressing data breaches or other incidents would be essential. The treaty would establish accountability mechanisms to ensure that data embassies meet high standards of governance, security, and incident response. For example, data embassies could be required to appoint designated data controllers responsible for ensuring compliance with international privacy regulations and responding to potential breaches. If breaches occur, there would be a predefined process for notifying affected parties and mitigating damage, ensuring embassies are held accountable for any failures in security or data protection.

By codifying these elements into an international treaty, the global community could establish a legal and operational foundation for data embassies that transcends national borders, allowing data to flow more freely while ensuring its security and privacy. This framework would not only promote global cooperation on data governance but also help to create a more secure digital economy, where trust in cross-border data transfers is the norm rather than the exception.

The success of a global treaty on data embassies would depend on the commitment of participating nations to uphold its principles and engage in meaningful international collaboration. Just as treaties have been successful in areas like arms control and environmental protection, a well-designed treaty for data embassies could pave the way for a more cohesive and trusted global data infrastructure.

8. Conclusion: A New Frontier for Data Governance

The digital economy thrives on the free, secure flow of data, powering innovation, global commerce, and international cooperation, yet current governance frameworks struggle to keep pace with the challenges of globalization and data sovereignty. Data embassies offer a groundbreaking solution by creating legally neutral spaces that transcend national boundaries, providing a framework that respects both individual privacy rights and national sovereignty. By granting data centers a status akin to diplomatic embassies, they enable secure cross-border data transfers under the jurisdiction of the home country rather than the host country, eliminating legal uncertainties that often impede international transactions.

Despite promising prospects, significant challenges remain, including governments' resistance to relinquishing control over data stored within their borders and the wide disparity in privacy standards across countries. However, these hurdles could be addressed through robust international oversight mechanisms and the establishment of global privacy standards based on frameworks like the GDPR. The potential of data embassies to create a more secure, transparent, and cooperative global data economy is immense, offering a transformative approach to data governance

that could revolutionize how we handle digital assets in an increasingly interconnected world.

Works Cited

"Data embassies in India: The future of data diplomacy and privacy." One Young India, www.oneyoungindia.com/cuet-and-upsc-general-studies-notes/data-embassies-in-india-the-future-of-data-diplomacy-privacy. Accessed 27 Dec. 2024.

Basu, Arindrajit [Datasphere Initiative]. "How data embassies can promote data security for all." Medium, 3 Aug. 2023, medium.com/@thedatasphere/how-data-embassies-can-promote-data-security-for-all-57bc523146b7.

Court of Justice of the European Union. Schrems II: Judgement in Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, 16 July 2020, https://curia.europa.eu/jcms/jcms/j_6/en/.

Culver, Clifford. Data Sovereignty: The Impact of Digital Borders on the Cloud. Palgrave Macmillan, 2020.

Greenleaf, Graham. Asian Data Privacy Laws: Trade and Human Rights Perspectives. Oxford University Press, 2014, https://academic.oup.com/ijlit/article-abstract/23/3/322/783852?redirectedFrom=fulltext

India Press Agency. "India Emerges as a Global Center for Data Embassies." Newspack Live!, 21 Sept. 2024, live.ipanewspack.com/2024/09/india-emerges-as-global-center-for-data.html.

ISO/IEC 27001. Information Security Management Systems — Requirements. International Organization for Standardization, 2013.

Kharazishvili, Yu.M. & Kwilinski, Aleksy. (2023). Methodology for Determining the Limit Values of National Security Indicators Using. Virtual Economics. 5. 7-26. 10.34021/ve.2022.05.04(1).

Kolessova, Anna-Maria " Estonia's Data Embassy Initiative: A Framework for Building Cyber Resilience in Other Countries." (Masters Thesis) Tallin University of Technology 2023, https://digikogu.taltech.ee/et/Download/dae125ad-ef19-4f5b-b087-305bdfc2aed2.

Meyer, Thiébaut. "Data embassies: Strengthening resiliency with sovereignty." Google Cloud Blog, 12 Nov. 2022, cloud.google.com/blog/products/identity-

security/data-embassies-strengthening-resiliency-with-sovereignty.

Samanta, Ankit. “Data Sovereignty Laws: Managing Compliance Across Jurisdictions.” Neumetric, 9 Dec. 2024, www.neumetric.com/journal/data-sovereignty-laws.

Sarkar, Sandipan, and Sandipan Sarkar. “Living in a data sovereign world.” IBM Blog, 16 Oct. 2023, www.ibm.com/blog/living-in-a-data-sovereign-world.

Schwartz, Paul M. "Global Data Privacy: The EU Way."New York University Law Review, vol. 94, 2019, pp. 771–814.

Shrivastava A and Lakra R, Diplomatic Law Reimagined? Appraising the Risks and Prospects of Data Embassies, Law School Policy Review, 2024, https://lawschoolpolicyreview.com/2024/01/23/diplomatic-law-reimagined-appraising-the-risks-and-prospects-of-data-embassies/

TONOMUS NEOM Hub . “Data Sovereignty and Geopolitical Implications for Cloud Services.” Tonomous Neom, 1 Oct. 2024, tonomus.neom.com/en-us/insights/data-sovereignty-and-geopolitical-implications-for-cloud-services.

Data Breach Management: Key Considerations in Designing an Effective Prevention, Response and Remediation Plan

Adeolu Idowu and Sumbo Akintola
Aluko & Oyebode

Abstract

Data breaches pose a significant and escalating threat in today's digital world, often compromising personal, financial, and organisational information with sometimes severe outcomes such as privacy violations, reputational damage, identity theft, financial loss and national security risks. As cyber-attacks grow in frequency and sophistication, robust strategies are required to avoid or mitigate their impact. The connection between data privacy and protection and the critical imperative to prevent data breaches is reflected in the Nigeria Data Protection Act (NDP Act), which mandates data controllers and processors to implement measures ensuring the security, integrity, and confidentiality of personal data, protecting against unauthorised access, misuse, and loss. Preventing data breaches is a critical element of data protection and an effective data protection regime must be focused on preventing, responding to and remediating data breaches. This article examines the types and causes of data breaches, principles of effective management, and preventive measures aligned with legal and best practice standards. It also highlights the importance of post-breach remediation, continuous improvement, and incident learning to safeguard organisations and stakeholders from the devas-

tating effects of data breaches.

Keywords: Data, Breach, Prevention, Response, Remediation

1. Introduction: Overview of Data Breaches

A data breach is the intentional or inadvertent exposure of confidential information to unauthorised parties (Cheng et al. 1). It is an unauthorised access, disclosure, or theft of sensitive, confidential, or protected information, resulting in potential harm to individuals, organisations or nations. Data breaches have existed as long as individuals or companies store or maintain records of private information in any form, including paper (Groot). Given advancements in the digital economy worldwide and the rapid development of related technologies, such as 5G and artificial intelligence, data has become an important resource globally, however, a plethora of potential risks of data breaches accompany such developments in information technology (Li et al. 2).

According to the Nigeria Data Protection Act, 2023 (NDP Act), personal data breach is a breach of security of a data controller or data processor leading to or likely to lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. While the legal definitions may vary in different jurisdictions, the concept of a data breach is consistent across board.

Data breach can take many forms, from simple loss or theft of physical documents and portable devices (Hammouchi et al. 1005) to more sophisticated cyber-attacks involving compromised servers, email accounts, or social media profiles. It may also include the theft of devices or advanced persistent threats that involve long-term, targeted attacks on an organisation's systems.

2 Causes of Data Breaches

Data breaches mostly stem from preventable factors that often involve human errors, organisational shortcomings including weak internal controls, and vulnerabilities introduced by third-party relationships.

Human error or malicious actions by individuals are the most critical leading causes of data breaches. They are the intentional or unintentional actions/inactions of employees and users that cause, spread or allow a security breach. Some of these errors include data handling mistakes, weak or reused passwords, failure to apply security patches, falling victim to phishing attacks, inadvertent disclosure of private or sensitive information, improper use of personal devices, unauthorised application, installation, and improper disposal of data.

A lack of organisational practices, policies, procedures and security protocols also play a significant role in the occurrence of data breaches. Some organisational factors that can cause data breaches include backdoor and application vulnerabilities, weak security policies and procedures, lack or inadequacy of employee training, poor access controls and user authentication as well as inadequate data encryption and storage.

Third-party vendors, contractors, and service providers are often linked to data breaches where proper and necessary precautions are not implemented. Common third-party related causes include engaging third parties without effective due diligence in selection or onboarding, operating with inadequate data security measures that expose the organisation where there is a security failure, and poor contractual and legal safeguards. Data controllers and processors must ensure that the third party processors they engage are properly onboarded and made aware of the need to maintain the integrity of the personal data of data subjects. The NDP Act also imposes a responsibility on data controllers and processors who engage third party processors to ensure that they comply with the provisions of the NDP Act and adherence to these provi-

sions will generally reduce the risk of data breaches by such third-party processors that will impact the data controllers and processors. The obligation for third party risk management is not unique to Nigeria, and applies across jurisdictions. For instance, Articles 24 and 28 of the European Union General Data Protection Regulation (EU GDPR) provide for the responsibility of a data controller to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the EU GDPR and ensures the protection of the rights of data subjects.

3 Types of Data Breaches

There are various types of data breaches , and their frequency and impact continue to grow. According to the United Kingdom Data Breach Report 2024, phishing attacks were the most prevalent, affecting 84% of businesses. These attacks are followed by breaches where cybercriminals impersonate organisations via emails or websites, and viruses or other forms of malware. Some of the types of data breaches include:

1. Phishing Attack (Houghton): This is one of the most common and effective methods used to steal sensitive information. Typically, in phishing attacks, attackers install malware on the victim's device, allowing them to access data or obtain sensitive information that can be sold on the dark web (Zlatolas et al. 8642). Phishing is responsible for 15% of all data breaches and remains a favoured technique among attackers due to its simplicity and effectiveness (Kosinski). There are **several variations of phishing attacks, such as:**

   a. Bulk email phishing, where attackers send spam emails to many recipients with the intent that targets will fall victim. These emails often mimic legitimate communications from well-known organisations by using official logos and branding to increase their credibility.

b. Spear phishing: This is a more targeted form of phishing where the attacker focuses on a specific individual. The victim is typically someone with a certain level of authority or has access to sensitive information that the attacker can exploit. When spear phishing is directed at high-profile individuals, such as executives or wealthy targets, it is often referred to as "whale phishing" or a "whaling attack".

   Another form of spear phishing attack is business email compromise (BEC) and is specifically aimed at stealing money or valuable information from a business or organisation. This can include sensitive data such as trade secrets, customer information, or financial records. In BEC attacks, cybercriminals usually impersonate high-ranking executives or trusted business partners to trick employees into transferring funds or sharing confidential information.

c. Vishing (Voice Phishing): Vishing refers to phishing attacks conducted over the phone. Cybercriminals use caller ID spoofing to make their calls appear as though they are from legitimate organisations, such as banks or government agencies. According to the Anti-Phishing Working Group (APWG), vishing incidents increased by 260% between 2022 and 2023, highlighting the growing threat of voice-based phishing attacks (APWG).

d. Social Media Phishing: Social media phishing leverages platforms like Facebook, LinkedIn, and X (formerly Twitter) to deceive users into revealing personal information. Scammers use direct messages or platform-specific messaging systems to impersonate legitimate entities or individuals and lure victims into providing sensitive details.

2. Malicious Software (Malware) Attacks: A malware is any type of software designed to harm or exploit a computer's system. A malware is often loaded onto a system by users without intent, providing hackers with access to a computer's system and poten-

tially connected systems. According to Statista (Petrosyan) there were 6.06 million malware attacks globally in 2023.

Ransomware is a type of malware that encrypts an individual's files or private data and demands payment to provide the decryption key. A ransomware data breach can stall business operations and may result in identity theft, intellectual property theft, financial losses, data breach costs and reputational damage (National Cyber Security Centre). Some ransomware will also try to spread to other machines on the network, such as the Wannacry malware that impacted the United Kingdom National Health Service in May 2017 (L).

3. Physical Theft: Physical theft of devices that contain sensitive or valuable information can pose significant security risks that may lead to a data breach. This threat is especially prominent for employees who work remotely or frequently travel, as their devices are more likely to be exposed to theft of both personal and organisational information.

4. Social Engineering: Social engineering is a type of psychological manipulation where threat actors get people to divulge secure sensitive information. An attacker uses social skills to compromise an individual or organisation's credentials for malicious purposes. According to Verizon's report, 68% of breaches involve a non-malicious human element, like a person falling victim to a social engineering attack or making an error (Verizon Business).

4 Local and Global Incidents of Data Breach and Associated Financial and Other Implications

4.1 Instances of Data Breach in Nigeria

The Nigeria Data Protection Commission (NDPC) reported that its main areas of investigation during the year 2019 - 2020 included data breaches (Nigeria Information Technology Development

Agency). In March 2024, the NDPC noted that it had realised over N400,000,000 in revenue from penalising cases of data breaches in the digital space, while making a commitment to the continued protection of Nigerian citizens' data (Mom). Additionally, it was stated that the NDPC had received over 3,000 complaints and had fined individuals and institutions that had defaulted in implementing data protection measures (Mom). Some specific instances of data breach or alleged data breach in Nigeria include:

1. Lagos State Internal Revenue Services (LIRS)

One of the first fines issued by the NDPC under the NDPR was a fine of N1,000,000 on Lagos State Internal Revenue Services in relation to a breach of taxpayer information(NDPC). The LIRS was found to have exposed the personal data of some taxpayers in the process of harmonising historical tax data.

2. National Identity Management Commission (NIMC)

In June 2024, Paradigm Initiative (PI), a pan-African social enterprise raised an alarm over the breach of data of Nigerians domiciled at the National Identity Management Commission (NIMC) (Vanguard). PI alleged that the National Identification Numbers (NIN), Bank Verification Numbers (BVN) and other personal data of Nigerians were sold for as low as N100 on unauthorised websites (Aro). The NIMC denied the allegations and after investigations by the NDPC, were not found liable or awarded any fines or other penalties, however, the allegations raised doubts about the integrity of the security measures employed by NIMC to protect the personal data of Nigerians within its products and service ecosystem, and its technological infrastructure

Organisations must note that the imposition of fines by regulators where there is a data breach are not the only consequence of data breaches. For publicly traded companies in mature economies, it is reported that there is an average decline of 7.5% in their stock value after a data breach; and that on average, it took 46 days for their stock prices to return to pre-breach levels (Huang et al.).

These are outside the other direct costs of data breaches which include audit and legal fees, revenue lost to business downtime and, in some cases, ransomware fees, which have in some instances bankrupted organisations. In some jurisdictions, credit-ratings may also be impacted by an organisation's history of data breaches resulting in higher borrowing costs for such organisations (Huang et al.).

A data controller or data processor may also become liable to pay damages or compensation pursuant to civil proceedings brought by a data subject who suffers any loss as a result of data breach where it is shown that such breach arose from a violation of the obligations of the data controller or data processor under the NDP Act.

4.2 Instance of International Data Breaches

British Airways

British Airways (BA) suffered a data breach in 2018 when its systems were compromised by attackers and then modified to harvest customers' details as they were inputted (Tidy). The stolen data included login details, payment cards and travel booking details as well as names and addresses. A subsequent investigation revealed that sufficient security measures, such as multi-factor authentication, were not in place at the time of the breach. BA was ultimately fined by the Information Commissioners Office (ICO) for the data breach which affected more than 400,000 of its customers (Information Commission Office).

The consequences of data breaches may also extend to criminal liability. This may occur where a data controller or data processor fails to comply with orders issued by the regulator in the wake of a data breach. Under the NDP Act, a data controller or data processor is liable, upon conviction, to a fine or imprisonment for a term of not more than one year or both.

5. Measures to Prevent Data Breaches

Recognising that data breaches pose significant risks to business operations and government services, it is critical that organisations identify, assess and understand the various channels in their systems, processes and activities where a data breach can occur and deploy standard technical and organisational measures to prevent the occurrence of data breaches as much as possible and safeguard personal data. Specifically, the following measures can be implemented by organisations to prevent data breaches:

a. Data Encryption: Encryption is one of the ways of safeguarding personal data, as it ensures that data cannot be decoded without authorised access.

b. Pseudonymisation: Organisations may implement pseudonymisation or other methods of de-identification of personal data to reduce risk of data breaches.

c. Regular Security Audits and Assessments: Organisations must carry out regular security audits on their systems, processes and activities to identify weaknesses and implement any remedial actions. This may include assessing the effectiveness and adequacy of existing security measures, adhering to organisational policies on data privacy and protection, among others.

d. SecureAccess Control: Organisations must implement strong access control mechanisms (Zhang et al. 433). Access to data must be limited to employees and authorised third parties that require those specific data to carry out specific functions. This will reduce the possibility of illegal data access and data breach. Additionally, access permissions should be reviewed regularly to ensure that only relevant personnel have access to personal data in the organisation's possession.

e. Employee Training and Awareness: One of the obligations of data controllers under the NDP Act and the NDPR (alto-

gether the "Nigeria Data Regulatory Instruments") is to conduct regular training of employees on data protection. Organisations must provide employees with adequate information and training on data breach prevention, the importance of safeguarding personal data and steps to take where a breach has occurred. Where employees have the adequate information and are committed to safeguarding personal data, this can significantly reduce the risk of data breaches or its impact if a data breach occurs. Additionally, employees must have not only good awareness, but also good practices in handling of data (Zhang et al. 434).

f. Risk Mitigation Plan: Pursuant to the provisions of the NDP Act, organisations must have a Risk Mitigation Plan (RMP) that addresses the prevention of data breaches and reduction of the impact of such data breach if it occurs. The RMP must specify the processes to implement and ensue the security, integrity, confidentiality, availability and resilience of processing systems and services. Organisations may deploy multi-factor authentication for all employees as well as threat detection tools to reduce the potential occurrence of data breach within the organisation. Additionally, the RMP should provide for processes to restore availability and access to personal data in a timely manner in the event of a physical or technical incident. Lastly, organisations must ensure regular updating of technical and organisational measures as well as introduction of new measures to address shortcomings in effectiveness and to accommodate evolving risks.

6. Building an Effective Response Plan in Line with Legal Requirements and Best Practices

An effective data breach response plan is crucial for mitigating the impact of data breaches and ensuring compliance with legal re-

quirements. Having an effective data breach response plan ensures that the breach is contained and that the harm caused by the breach is managed adequately to prevent further harm. In developing an effective response plan, it is important to consider Nigerian laws on the subject as well as global best practices.

The Nigeria Data Protection Regulatory Instruments provide a legal framework for data protection and make provisions for the actions to be taken in the case of a data breach. These provisions mandate organisations to implement robust measures for data security and breach management. The quality of a good data breach response plan will be measured by the extent to which it is able to minimise the consequences of a breach.

6.1 Elements of a Good Response Plan

Ultimately, the goal of a response plan is to ensure that the organisation recovers from the data breaches quickly and with the least amount of damage whether legal or regulatory, reputational and/or financial. To build an effective data breach response plan, organisations must therefore consider and document the following in their relevant policies and frameworks:

1. Implementation of tools and processes for the early detection of a data breach: In the event that a data breach still occurs despite all the preventive measures put in place by an organisation, it is important that there are tools in place for early detection and monitoring of the breach. This ensures that remediation activities kick-off early enough to avoid further harm to the data due to the breach.
2. Establishment of a response team and responsibilities: Organisations should constitute a data breach response team and clearly identify members' roles. How an organisation chooses to structure its data breach response team will

depend largely on the nature of the business and the industry within which it operates. However, it is necessary that there are members within the team with knowledge of the provisions of the law regarding data breaches, people with the technical skill set to identify the root cause(s) of data breaches, stalling its spread and rebooting affected systems and devices, where applicable as well as leadership executives and communication experts (DeVoe and Rahman 15-16).

Assembling a comprehensive data breach response team ensures that the organisation manages the breach effectively.

3. Assessment of the data breach incident: It is important that immediately a breach occurs, the response team evaluates the extent and impact of the breach to determine what data was compromised, how the breach occurred and its potential consequences.

4. Notification obligations: The NDP Act places an obligation on the data processor to, upon being aware of the breach to the personal data, immediately notify the data controller of such breach, and describe the nature of the personal data breach. Additionally, where the breach is *likely to result in a risk to the rights and freedoms of individuals*, the data controller is expected to notify the Nigeria Data Protection Commission (NDPC) and the affected data subject, within 72 hours of becoming aware of the breach.

   The European Union's General Data Protection Regulation (GDPR) has a similar provision that places an obligation on all organisations to notify the ICO of all data breaches unless they can demonstrate that the breach is unlikely to result in a risk to rights or freedom (BreachRX).All states in the United States of America have enacted legislations re-

quiring notification of personal data breaches to the relevant data protection authority (Federal Trade Commission).

These provisions across various jurisdictions underscore the importance of reporting any potential and actual data breach. Notification of any data breach to affected individuals is especially important as it provides the opportunity for the individuals to limit the extent of their exposure in the most practicable way. For example, where there has been a breach of the account information of a data subject, notice to the data subject may afford the individual the opportunity to inform other parties who may be transacting with such individual, informing them of the dangers of dealing with the exposed account.

5. Effective communication plan: Organisations must incorporate robust communication into their strategies to mitigate the impact of the data breach and guide stakeholders through the incident while occurring and in its aftermath. In addition to determining the appropriate type of response, organisations must also understand how to transmit their response to the public and communicate with the stakeholders effectively (Nikkhah 3).The data breach response team may also prepare templates for communicating with affected individuals, regulators, and other relevant stakeholders. Transparency and timely updates help maintain good public perception and improve stakeholder confidence.

Through a comprehensive approach that integrates legal compliance, leverages technology and best practices, organisations can better safeguard their data assets and mitigate the impact of breaches, ultimately fostering a more secure and resilient digital ecosystem.

6.2 Post-Breach Remediation Plan: Steps to Take after a Data Breach

Once the immediate response to a data breach is underway, it is crucial to address the root causes and prevent future incidents. The steps outlined below may be considered following the occurrence of a data breach:

1. Policy Review and Updates: An organisation that has suffered a data breach must conduct a thorough review of existing data protection policies to identify any gaps or weaknesses that contributed to the breach. This assessment should be comprehensive, covering both technical and procedural aspects. Based on the lessons learned from the breach, the policies may be updated to address identified weaknesses. The updated policies should be in line with the provisions of the extant laws and regulations of the country where such an organisation operates and should be communicated clearly to all employees.
2. Training and Awareness Programs: Regular training sessions should be conducted for employees, focusing on data protection best practices and their responsibilities under the updated policies. Training helps in building a culture of security awareness within the organisation. Organisations should use case studies from previous incidents to conduct specific training that provide learnings that will prevent reoccurrence and strengthen future operations. These sessions should detail the causes, the impact on the organisation, and the corrective actions being implemented. Such trainings should ensure that employees are aware of the vulnerabilities that led to the breach and are equipped to prevent similar incidents in the future. The organisation should also implement recurrent awareness campaigns to keep data protection top of mind for all staff members. These campaigns can include workshops, new-

sletters, webinars and frequent reminders on the importance of data security.

3. Feedback Procedure: Organisations may also establish a feedback procedure to be notified of any vulnerability or breach and for the purpose of continuous improvement of the remediation processes where a breach has occurred. This can include regular reviews of the response plan, incorporating lessons learned, and proactively adopting best ways to guard or mitigate against threats and evolving tactics used by criminals.

By meticulously adhering to the provisions of applicable laws and regulations on data protection and incorporating evolving global best practices, organisations can build resilient data breach management systems that not only address breaches effectively but also fortify their overall data protection strategies. This comprehensive approach ensures that organisations are prepared to respond to breaches promptly, minimise their impact, and prevent future incidents.

7. Conclusion

The increasing sophistication of cyber-attacks necessitates a robust and proactive approach to data breach management. Designing an effective data breach management and response plan requires a comprehensive approach that cuts across the identification of all touchpoints and processes where a data breach may occur, implementation of prevention measures for the identified areas of breach, mode of response where there has been a breach, and deployment of remedial steps to address the breach and prevent a recurrence. This significantly reduces an organisation's risk of exposure.

Prevention starts with robust technical, operational and cybersecurity measures, employee training, and proactive risk assess-

ments to minimize vulnerabilities. It is pertinent to note that all organisations can suffer data breaches, though the size, frequency, nature and impact of the breaches will vary. Consequently, it is an organisational imperative to develop an efficient and effective response plan which is critical to limiting damage and ensuring swift recovery. By integrating the elements enumerated in this article and converting same into a cohesive framework, organisations will not only avoid or mitigate the impact of data breaches but also enhance their resilience and safeguard their reputation in an increasingly complex digital landscape.

Works Cited

Aro, Busola "Investigation Ongoing – Bosun Tijani Speaks on Alleged NIMC Data Breach" The Cable, 2024, https://www.thecable.ng/investigation-ongoing-bosun-tijani-speaks-on-alleged-nimc-data-breach/ accessed 16 November 2024

Cheng, Long, et al "Enterprise Data Breach: Causes, Challenges, Prevention and Future Directions" Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. vol 2017 pp. 1-14, doi: 10.1002/widm.1211

"Cyber Security Breaches Survey 2024" Department for Science, Innovation and Technology, 2024, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024 accessed 08 November 2024

"Data Breach Response: A Guide for Business" Federal Trade Commission, 2021, "Data Breach Response: A Guide for Business" Federal Trade Commission, 2021, https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business accessed 16 November 2024

De Groot "The History of Data Breaches" Digital Guardian, 2019, J. De Groot, "The History of Data Breaches, Digital Guardian" 2019 [Online] available at https://digitalguardian.com/blog/history-data-breaches accessed on 07 November 2024

DeVoe, Charles and Shawon Rahman "Incident Response plan for a Small to Medium Sized Hospital" International Journal of Network Security & its Applications vol. 5, no. 2, 2013, 1-20, ResearchGate, doi:10.5121/ijnsa.2013.5201

Hammouchi, Hicham, et al "Digging Deeper into Data Breaches: An Exploratory Data Analysis of Hacking Breaches over Time" Procedia Computer Science vol. 151, 2019, pp. 1004-1009

Houghton, Sean "Types of Data Breaches Every Business Must Know" Aztech, 2024, 13 Common Types of Data Breaches Every Business Must Know accessed 08 November 2024

Huang, Keman et al. "The Devastating Business Impacts of a Cyber Breach" Harvard Business Review, 2023, https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach accessed 08 November 2024

"Mitigating Malware and Ransomware Attacks" National Cyber Security Centre, 2021, https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks accessed 05 November 2024

Nikkhah, Hamid "Strategising Responses to Data Breaches: A Multi-Method Study of Organisational Responsibility and Effective Communication with Stakeholders" International Journal of Management Information Systems, 2024

Kosinski, Matthew "Cost of a Data Breach Report 2024" IBM, 2024, Cost of a data breach 2024 | IBM accessed 08 November 2024

L, Jon "WannaCry Ransomware: Guidance Updates" National Cyber Security Centre, 2017, https://www.ncsc.gov.uk/blog-post/wannacry-ransomware-guidance-updates accessed 05 November 2024

Li, Jin, et al "Data Security Crisis in Universities: Identification of Key Factors Affecting Data Breach Incidents" Humanities and Social Sciences Communications, vol. 10, no. 207, 2023, pp. 1-18, doi.org/10.1057/s41599-023-01757-0

Mom, Claire "NDPC: Over N400m Realised from Penalising Data Breaches in Less than Two Years" The Cable, 2024, https://www.thecable.ng/ndpc-over-n400m-realised-from-penalising-data-breaches-in-less-than-two-years/ accessed 15 November 2024

"Nigeria Data Protection Regulation Performance Report (2019-2020)" Nigeria Information Technology Development Agency, 2020, https://ndpc.gov.ng/resources/# accessed 08 November 2024

"Penalty Notice, Section 155, Data Protection Act 2018" Information Commissioner's Office, 2020, https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf accessed 08 November 2024

Petrosyan, Ani "Annual Number of Malware Attacks Worldwide from 2015 to 2023" Statista, 2024, https://www.statista.com/statistics/873097/malware-attacks-

per-year-worldwide/ accessed 07 November 2024

"Phishing Activity Trends Report, 4th Quarter 2023" APWG, Unifying the Global Response to Cybercrime, 2024, https://docs.apwg.org/reports/apwg_trends_report_q4_2023.pdf accessed 07 November 2024

"The United Kingdom Data Protection Laws' Incident Response Guidelines- How to Prepare your Organisation for Compliance with the Data Protection Act 2018 and UK GDPR" BreachRX, https://www.breachrx.com/global-regulations-data-privacy-laws/united-kingdom-data-protection-laws/ accessed 16 November 2024

Tidy, Joe "British Airways Fined 20m over Data Breach" BBC, 2020, https://www.bbc.com/news/technology-54568784 accessed 16 November 2024

Zhang, Xichen, et al "Data Breach: Analysis, countermeasures and challenges" International Journal of Information and Computer Security vol. 19, 2022, nos. 3/4 2022

Zlatolas, Lili, et al "Data Breaches in Healthcare: Security Mechanisms for Attack Mitigation" Cluster Computing, vol. 27, 2024, pp. 8639-8654, doi.org/10.1007/s10586-024-04507-2

Creative Advocacy as a Catalyst for Privacy-Conscious Behaviors

Dodeye Ebri
Public and Private Development Centre (PPDC)

Abstract

The proliferation of digital technologies has introduced unprecedented challenges to data privacy, requiring innovative strategies to foster privacy-conscious behaviors. While traditional privacy awareness campaigns often fail to resonate due to vague messaging and one-size-fits-all approaches, creative advocacy offers a transformative solution. This paper explores how innovative methods such as interactive campaigns, digital storytelling, and gamification can bridge the gap between complex privacy concepts and practical understanding. Drawing on theoretical models like the Health Belief Model and Social Cognitive Theory, it highlights how creative advocacy enhances user engagement, contextualizes privacy risks, and promotes sustainable behavior change. Case studies demonstrate its effectiveness in diverse contexts, particularly for audiences with varying levels of digital literacy. The paper also examines the relationship between awareness and privacy-conscious behaviors, emphasizing the need for targeted, relatable, and culturally sensitive initiatives to address the evolving digital ecosystem. Finally, it argues that creative advocacy is not merely an alternative but a necessary approach to fostering a culture of data protection in the digital age.

Keywords: Creative Advocacy, Data Privacy, Privacy-Conscious Behaviors, Digital Literacy, Awareness Campaigns.

1. Introduction

The digital age has revolutionized how individuals interact, work, and live, but it has also introduced significant challenges regarding data privacy. With an estimated 5.52 billion internet users as of October 2024 comprising 67.5% of the global population, data sharing and digital footprints have become unavoidable aspects of modern life. Social media accounts for 5.22 billion active users illustrating the extent of personal data exchanged online (Petrosyan). This data exposure, often through routine activities such as browsing and online shopping, leaves users vulnerable to data misuse and privacy breaches.

Despite the recognized importance of data privacy being defined as the ability of individuals to control the collection, use, and distribution of their personal information online ("Understanding Privacy in the Digital Age - IEEE Digital Privacy") many users remain unaware of how their data is managed. This gap is further compounded by the complexities of understanding information privacy, communication privacy, and individual privacy. The interplay of these elements and ineffective awareness strategies contribute to an environment where data protection is not adequately prioritized. Existing awareness initiatives frequently fall short due to vague messaging, lack of relatable content, and the absence of targeted programs considering diverse digital literacy levels and cultural nuances across populations.

The limitations of conventional awareness methods underscore the need for innovative approaches to engage users and instill privacy-conscious behaviors. Programs that rely solely on traditional information dissemination often fail to resonate with users, particularly in regions with emerging digital ecosystems. This paper will explore how creative advocacy can serve as an effective driver for promoting privacy-conscious behavior, emphasizing its role as a bridge between complex data privacy concepts and practical user understanding. Through an analysis of innovative strat-

egies, case studies, and real-world challenges, this paper aims to illustrate that awareness, when delivered through creative and relatable advocacy, is essential for fostering a culture of data protection and responsible digital practices.

2. Literature Review

Awareness and education are crucial first lines of defense against cybercrimes and privacy violations (Eluwah 3). Over the past decade, research on factors influencing privacy behavior has grown significantly. Researchers, software developers, information security providers, and individuals have explored ways to enhance the privacy behaviors of ICT users. While ICT users claim to value their data privacy, they often disclose significant amounts of personal information when using internet-connected devices (Paspatis and Tsohou 396-415).

Tilburg University underscores the importance of privacy awareness, stating, “Privacy is a very topical issue, increasingly so. Students and staff are increasingly impacted by it and are more aware of the risks and dangers if things go wrong. The more people are aware, at all levels of the organization, the better we can do the right things to carefully process and protect our data.

2.1 Gaps in Conventional Approaches

Conventional awareness methods in the context of data privacy have faced significant challenges, particularly in addressing the complexities of digital literacy and user engagement. Traditional approaches, which often rely on general awareness campaigns and one-size-fits-all messaging, have struggled to effectively convey the importance of personal data protection to diverse populations. A study by Paspatis et al., (76) highlights that despite an increasing volume of privacy awareness initiatives, many fail to re-

sonate with the target audience due to ambiguity in the language, generic messaging, and a lack of relatability to users' specific needs. Furthermore, conventional efforts often focus on disseminating information through passive means, such as one-time informational flyers or broad media campaigns, which do not foster deeper engagement or lasting behavior change.

Additionally, many of these traditional campaigns do not account for the varied levels of digital literacy across populations, leading to a gap in understanding, especially in regions with emerging digital ecosystems (Park 215-236). Users may feel overwhelmed by the sheer volume of privacy information, leading to confusion about protecting their data online. This highlights the need for more targeted, interactive, and contextually relevant privacy education.

2.2 Key Theoretical Models

Several theoretical models can support the impact of creative advocacy on behavior change, particularly when addressing privacy-conscious behaviors. The Health Belief Model (HBM), which has been widely used in health campaigns, posits that individuals are more likely to engage in protective behaviors if they perceive a significant threat to their well-being and believe they can take effective action (Rosenstock 354-386). Creative advocacy can amplify these perceptions by framing privacy risks in more relatable and immediate terms, thus making privacy protection feel more urgent and actionable.

Another relevant theory is the Social Cognitive Theory (SCT), which emphasizes the role of observational learning and the influence of social norms on behavior (Locke 169-171). For instance, campaigns that showcase influencers or celebrities adopting privacy-conscious practices may encourage others to follow suit, creating a ripple effect that spreads privacy awareness.

3. Understanding Creative Advocacy

Creative advocacy is an approach to awareness campaigns that employ innovative, engaging, and often unconventional methods to convey critical messages. Unlike traditional approaches, which typically rely on static information dissemination through text-heavy flyers or generic advertisements, creative advocacy uses emotional appeal, interactive media, storytelling, and visual art to capture attention and make complex issues more relatable. The goal is not only to inform but to inspire behavior change through engagement and resonance with the audience's everyday experiences and values.

In the context of data privacy, creative advocacy can play a transformative role in shifting users' attitudes and behaviors regarding how they manage their personal information online. Data privacy is a highly complex issue that requires an understanding of digital rights, the implications of data sharing during data collection, and the risks of data misuse. A creative advocacy approach can break down these complexities into digestible, relatable content, often using real-world examples, engaging visuals, and interactive formats. Infographics, viral videos, and social media campaigns that highlight the risks of sharing personal data online can directly appeal to users' emotions, helping them recognize the importance of safeguarding their information. The aforementioned strategies can be applied to data privacy, where a fresh approach can make individuals more aware of the privacy risks they face and encourage them to take action to protect their personal data.

3.1 The Role of Creative Advocacy

Creative advocacy has proven to be an effective tool for awareness campaigns in other fields, such as public health and environmental protection, and it offers valuable insights for promoting privacy-conscious behavior. The "Truth" campaign, which

aimed to reduce smoking rates among young people, is a notable example. It utilized bold, innovative advertising that captured attention through humor and stark visuals, resulting in significant shifts in attitudes toward smoking. This approach helped convey important health risks in a way that was both engaging and easy to understand, making it a powerful tool for behavior change.

Creative advocacy often involves crafting messages that are both persuasive and memorable, utilizing platforms and formats that align with the target audience's interests and everyday experiences (Lee and Kotler 1494-1517). This strategy could be highly effective in raising awareness about data privacy, particularly when reaching younger, digitally native users who may be less responsive to traditional methods.

4. Why Creative Methods Are Necessary for Capturing Digital Audiences

As the digital world continues to evolve, so too must the methods used to engage with audiences. Traditional awareness campaigns often fall short in capturing the attention of digital-native users, particularly younger generations who are increasingly inundated with information online. Creative advocacy methods, such as interactive campaigns, gamification, and storytelling, offer a way to break through the noise. These methods are designed not only to capture attention but also to keep audiences engaged long enough for them to process key information. For example, interactive online quizzes, gamified learning platforms, and engaging videos allow users to actively participate in their learning process rather than passively consume information. According to Lee and Kotler (1494-1517), using creative formats that align with the interests and social behaviors of the target audience fosters deeper engagement and greater retention of information. Additionally, the rise of social media and influencer culture has made creative,

shareable content a vital tool for spreading awareness. Given the saturation of content in the digital space, relying solely on traditional awareness methods risks leaving vital privacy messages unheard.

4.1 Relationship between Awareness and Privacy Conscious Behaviors

There is substantial evidence supporting the idea that awareness plays a significant role in driving privacy-conscious behavior, particularly in the context of online interactions. Research by Ara et al., (93-110) found out that privacy-aware individuals tend to make more deliberate decisions when it comes to managing their personal information online. The more informed users are about the risks of data exposure, the more likely they are to leverage privacy features to safeguard their data.

However, as internet usage continues to grow, privacy awareness alone does not always translate into protective behavior. Belanger and Crossler (1017-1041) argue that the increasing dependence on digital platforms has rendered privacy calculus a method by which users weigh the risks and benefits of sharing personal information less effective. Consumers are often in a situation where they must disclose personal data to access essential services, regardless of their privacy concerns. This paradox highlights the limitations of privacy awareness in the face of modern technological ecosystems, where users are frequently coerced into sharing information due to the lack of alternatives.

Interestingly, Paspatis and Tsohou's (396-415) research reveals that, despite the pressures to share data, many digital natives are still highly aware of the risks associated with their online profiles. This translates to the fact that despite privacy awareness being widespread among some groups, it is unclear whether this awareness directly translates into privacy-conscious behavior further

suggesting that while awareness is a necessary first step, other factors such as digital literacy, platform design, and personal incentives also play a critical role in influencing behavior.

Furthermore, privacy consciousness defined as the degree to which an individual is aware of and concerned about their own and others' privacy, remains an important area of focus ("'Privacy Awareness Continues to Be Important in Personal Data Protection' | Tilburg University") . Privacy consciousness is not just about knowing the risks; it also involves being vigilant and proactive in safeguarding one's data. As a result, it is crucial to expand traditional privacy awareness training to include strategies for effectively applying that awareness in real-world online environments, particularly as more users engage in complex digital ecosystems.

5. Effective Creative Advocacy Strategies for Promoting Privacy-Conscious Behavior

Interactive Campaigns are powerful tools for engaging audiences in a way that passive media cannot. For example, quizzes or interactive web platforms that let users assess their online privacy knowledge and habits can effectively raise awareness. A study by Tasevski (7-22) demonstrated that when users are encouraged to interact with content that personalizes privacy risks, they show a greater understanding of privacy-related issues and are more likely to take protective measures. These campaigns also facilitate real-time feedback, providing an immediate educational experience that helps solidify privacy-conscious behavior.

Digital storytelling is another impactful strategy for promoting privacy awareness. This method not only informs but also emotionally resonates with the audience. Stories that showcase personal data mishaps or the consequences of inadequate privacy protections can help individuals understand the risks involved. Research by Crisan and Bortun (155-165) supports this approach,

arguing that storytelling is particularly effective in creating empathy, which can drive behavioral change. Storytelling especially when narrated and described using the language of the audience, creates an emotional connection, making privacy issues feel more immediate and personal, as opposed to abstract concepts.

Gamification of privacy education has proven to be an effective strategy, particularly for younger audiences. Gamified learning modules, such as those that reward users for achieving privacy goals or completing educational tasks, help sustain engagement while promoting awareness. Gamification provides a fun, interactive method for learning that encourages users to internalize privacy best practices through repetition and positive reinforcement.

Visual media, such as infographics, posters, and animations, play a crucial role in simplifying complex privacy concepts and making them more accessible. Visual representations of data breaches, the dangers of oversharing, and how personal data is used by third parties can help individuals quickly grasp the importance of data protection. According to a study by Das and Chakrabati (783-793), visual storytelling is highly effective in condensing large amounts of information into digestible, attention-grabbing formats. This method appeals to a wide audience, including those who might not engage with textual content. The immediacy of visuals makes privacy issues more relatable and easier to understand.

Social media platforms are indispensable in modern privacy advocacy, particularly given their widespread use. Creative privacy campaigns on platforms like Twitter, Facebook, and Instagram can utilize memes, challenges, and shareable content to engage users in conversations about data security. According to Gruzd and Hernández-García (418-428), social media offers an ideal space to reach large audiences, especially younger users who are often the most at risk for privacy violations. Using influencers or popular hashtags can help amplify the message and create a viral effect.

Furthermore, platforms like these allow for the dissemination of real-time updates about privacy risks, ensuring that the audience stays informed about emerging threats.

6. Examples of Successful Creative Advocacy Campaigns

Several creative advocacy campaigns have successfully engaged audiences and raised awareness about privacy issues, demonstrating the effectiveness of creative strategies in encouraging privacy-conscious behavior. One notable campaign is the **Delete Facebook** movement, which gained momentum following revelations about data misuse during the Cambridge Analytica scandal. This campaign leveraged social media platforms to encourage users to delete their Facebook accounts as a form of protest against the platform's handling of personal data. The **Your Data Your Rights** Campaign by the European Commission used a blend of digital storytelling and interactive elements to inform European Union citizens about their rights under the General Data Protection Regulation (GDPR). Through a series of visually engaging digital content pieces, including videos and social media posts, the campaign aimed to empower individuals to understand how their data was being collected and used. There is also, the **Privacy is Global** project by Heinrich Böll Stiftung using creative storytelling, including audio fiction, to explore data privacy issues in a relatable and engaging manner.

One radio drama series about data protection in Nigeria has proved to be effective in raising awareness and sparking conversations about data privacy, particularly among the target audience of individuals with limited prior knowledge. Key findings from focus group discussions and key informant interviews conducted during the launch of the drama series include a significant

increase in participants' understanding of data privacy issues, such as the government's right to surveillance and the role of service providers in protecting user data. The drama's use of relatable scenarios, such as the End SARS protests, resonated with participants, demonstrating the real-world impact of data privacy violations. The series was well-received, with participants and listeners praising its engaging storytelling, humor, and informative content. The drama inspired discussions and encouraged participants to take action, such as being more mindful of their online activities and advocating for stronger data protection laws.

The evidence from these case studies underscores the effectiveness of creative advocacy in promoting privacy-conscious behavior. While traditional methods may have limited success in engaging users and inciting behavioral change, creative campaigns leverage interactive, personalized, and emotional strategies to foster a deeper understanding of privacy risks. These approaches resonate with digital audiences and inspire action, making them critical tools in the ongoing effort to raise awareness about data privacy.

7. Challenges and Limitations of Creative Advocacy

While creative advocacy methods have proven effective in promoting privacy-conscious behaviors, several challenges and limitations need to be considered when implementing these strategies. Some of these limitations include; **resource constraints** as creative campaigns often require investments in multimedia production, skilled personnel, and digital platforms to ensure broad reach and engagement. Small organizations or those operating on limited budgets may struggle to design and execute campaigns with the level of creativity and interactivity needed to capture the

audience's attention. **Tailoring creative campaigns to diverse audiences** poses another challenge. Digital spaces host a broad range of demographics with varying levels of digital literacy, cultural backgrounds, and privacy concerns, which means that the same creative strategy may not be equally effective in all regions. This requires not only segmentation of the audience but also continuous adaptation of messages and formats to ensure inclusivity. Another critical challenge is **balancing clarity with creativity**. To engage audiences, creative campaigns often incorporate complex visuals, interactive elements, and innovative formats. However, there is a risk that these creative elements may obscure the core message, particularly when it comes to complex topics like data privacy. The challenge lies in ensuring that the message remains clear and understandable without diluting the creativity of the campaign.

These challenges highlight the need for thoughtful planning, resource allocation, and ongoing audience analysis when implementing creative advocacy strategies for privacy awareness. Addressing these limitations can help maximize the impact of creative campaigns and ensure they lead to meaningful behavior change.

8. Recommendations for Enhancing Creative Advocacy

To further enhance the effectiveness of creative advocacy in promoting privacy-conscious behaviors, several strategies can be implemented. One of the most powerful ways to expand the reach of creative advocacy is through **partnerships** with influencers and community advocates. These individuals or organizations often have established trust and credibility within specific audiences, which can significantly amplify the message. This strategy ensures that the message is not only heard but also resonates deeply with

diverse groups who may already follow these figures for other relevant causes. For creative advocacy to be truly effective, content creation must be **user-centric**, meaning it should be tailored to the needs, preferences, and concerns of the target audience. It is important to understand the digital behavior and privacy concerns of different groups to create content that speaks directly to them. This could involve using relatable scenarios, language, and formats that make complex privacy concepts easier to understand. For instance, incorporating storytelling, interactive videos, or memes that reflect real-world situations can help bridge the gap between technical jargon and everyday concerns. **Continuous improvement** in creative advocacy requires the integration of feedback mechanisms. These mechanisms allow for real-time evaluation of campaign effectiveness and enable advocates to adjust strategies based on user responses and experiences. This could involve conducting surveys, holding focus groups, or utilizing analytics to assess how well the audience is interacting with the content. Feedback mechanisms create a dynamic loop of engagement, where users feel heard and can contribute to the refinement of the advocacy approach.

9. Conclusion

This paper has explored the critical role that awareness plays in promoting privacy-conscious behaviors in the digital age. The increasing reliance on digital platforms has heightened the need for effective privacy education, yet traditional awareness campaigns often fall short due to gaps in engagement, lack of relatability, and limited reach. Through the analysis of research and theoretical frameworks, it has become clear that creative advocacy presents a promising approach to overcoming these challenges. When innovative strategies such as interactive campaigns, gamified learning, digital storytelling, and social media engagement,

are used, privacy awareness can be made more engaging and accessible to diverse digital audiences.

The findings underscore the importance of creative advocacy as an effective tool for not only raising awareness but also driving tangible behavior change. Creative approaches are particularly necessary in an era where conventional methods fail to connect with the diverse and dynamic needs of users across the globe. In light of these insights, stakeholders ranging from policymakers and privacy advocates to technology companies and educators must embrace and adopt creative strategies to promote privacy-conscious behavior. This call to action is not just for the benefit of individuals but for the broader protection of personal data in a constantly evolving digital landscape. Collaborative efforts to integrate creativity into privacy education will play a pivotal role in ensuring that users are equipped with the knowledge and tools to protect their digital identities.

Works Cited

Ara, Anjuman, et al. "The Effects of Privacy Awareness, Security Concerns and Trust on Information Sharing in Social Media among Public University Students in Selangor." International Business Education Journal, vol. 15, no. 2, 15 Dec. 2022, pp. 93–110, doi:10.37134/ibej.vol15.2.8.2022.

Bélanger, France, and Robert E Crossler. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems." MIS Quarterly, vol. 35, no. 4, 2011, p. 1017, doi:10.2307/41409971.

Crisan, Camelia, and Dumitru Bortun. "Exploring the Potential of Digital Stories as Tools for Advocacy." Digital Storytelling, 2017, pp. 155–165, doi:10.1057/978-1-137-59152-4_13.

Das, Bappa, and Debkumar Chakrabarti. "Image Is a Tangible Element of Visual Communication: Role of the Image to Increase Social Awareness." Smart Innovation, Systems and Technologies, 2021, pp. 783–793, doi:10.1007/978-981-16-0084-5_64.

Eluwah, Daniel. Cyber Awareness And Education In Nigeria: An Assessment, 12 Oct. 2021, p. 3, doi:10.13140/RG.2.2.23425.79202.

Gruzd, Anatoliy, and Ángel Hernández-García. "Privacy Concerns and Self-Disclosure in Private and Public Uses of Social Media." Cyberpsychology, Behavior, and Social Networking, vol. 21, no. 7, 1 July 2018, pp. 418–428, doi:10.1089/cyber.2017.0709.

Kotler, Philip, and Nancy Lee. Social Marketing: Changing Behaviors for Good. 6th ed., SAGE, 2016.

Lee, Nancy, and Philip Kotler. "Promotion: Deciding on Messages, Messengers, and Creative Strategies." Social Marketing: Behavior Change for Social Good, 6th ed., SAGE, Los Angeles, 2016, pp. 1494–1517.

Locke, Edwin A. "Social Foundations of Thought and Action: A Social-Cognitive Viewsocial Foundations of Thought and Action: A Social-Cognitive View, by Bandura Albert. Englewood Cliffs, NJ: Prentice-Hall, 1986, 617 Pp., Cloth." Academy of Management Review, vol. 12, no. 1, Jan. 1987, pp. 169–171, doi:10.5465/amr.1987.4306538.

Park, Yong Jin. "Digital Literacy and Privacy Behavior Online." Communication Research, vol. 40, no. 2, 23 Aug. 2011, pp. 215–236, doi:10.1177/0093650211418338.

Paspatis, Ioannis, and Aggeliki Tsohou. "How to Influence Privacy Behavior Using Cognitive Theory and Respective Determinant Factors." Journal of Cybersecurity and Privacy, vol. 3, no. 3, 17 July 2023, pp. 396–415, doi:10.3390/jcp3030020.

Paspatis, Ioannis, et al. "How Is Privacy Behavior Formulated? A Review of Current Research and Synthesis of Information Privacy Behavioral Factors." Multimodal Technologies and Interaction, vol. 7, no. 8, 29 July 2023, p. 76, doi:10.3390/mti7080076.

Petrosyan, Ani. "Internet and Social Media Users in the World 2024." Internet and Social Media Users in the World 2024, Statista, 5 Nov. 2024, www.statista.com/statistics/617136/digital-population-worldwide/. Accessed 25 Nov. 2024.

Rosenstock, Irwin M. "The Health Belief Model and Preventive Health Behavior." Health Education Monographs, vol. 2, no. 4, Dec. 1974, pp. 354–386, doi:10.1177/109019817400200405.

Tasevski, Predrag. "IT and Cyber Security Awareness – Raising Campaigns." Information & Security: An International Journal, vol. 34, 2016, pp. 7–22,

doi:10.11610/isij.3401.

Understanding Privacy in the Digital Age - IEEE Digital Privacy, digitalprivacy.ieee.org/publications/topics/understanding-privacy-in-the-digital-age. Accessed 25 Nov. 2024.

Deepfakes and Data Privacy: Navigating The Risks in the Age of AI

Motunrayo Adebayo
IPI Strategy Partners, Indiana Wesleyan University

Abstract

This paper attempts to investigate the impacts of deepfake technology, which is propelled by the emergence of artificial intelligence (AI). In the data privacy world, there has been significant concerns about the safety of information ecosystems, which has happened because of the enormous presence of fake information, in both audio and video formats in the information space, which are known as deepfakes. Deepfakes involve using synthetic media to make powerful machine learning algorithms, which could be deployed to produce fake audio/videos to wrongly inform individuals or general members of the public. The sharp rise in the growth of deepfake through Artificial Intelligence creates challenges while consumers of information try to identify genuine information from fake ones, this puts individuals at risk of exposure to issues such as identity theft, financial losses, general breach of personal privacy, and physical harm amongst others, while also compromising the integrity of data sources. This paper evaluates the rising implications of Deepfake technology on individual privacy and security, the level of adequacy of existing laws and frameworks in regulating such. Findings may support policymakers, information technology experts, and the public on response to the potential threats, and how to manage possible negative impacts.

Keywords: Deepfake, Artificial Intelligence, Data Privacy, Risk, Cybersecurity

1. Introduction

Technological advancements have increased astronomically in recent times, a major milestone was the introduction of Artificial intelligence (AI). The rapid growth of AI has further driven innovation on a global level, its impact affecting many industries and changing their daily activities. However, with the positive impacts of AI, there have also been negative implications. One of the dangerous impacts of AI has been the rise of deepfake technology. In simple terms, a deepfake is a piece of artificial media that uses false intelligence processes to either construct or edit an image, video, or audio recording in such a way that it portrays an event or a person wrongly (Kapoor, 2024). Mahashreshty (2023) also conceives deepfake as an artificial intelligence technology, which can create hyper-realistic media such as images and video. This made it possible to create audio or video of a real person saying and doing things he or she never said or did.

Information technology has improved very much in the last decade. Unfortunately, misapplications of technology have accompanied developments in the IT world. Deepfake can be highly deceiving and dangerous as it has a high potential to manipulate the public's opinions and their decision making. It is also causing problems in the lives of individuals, who have been victims of attempts to tarnish their brands. Oftentimes, deepfakes are usually targeted at political leaders, celebrities, and artists, however it could be used to cause damage to individuals. Deepfake technology can be used in creating bad videos/audios of a person as a form of bullying, revenge, and blackmailing tool. As technological advancement is inevitable, threats associated with its develop-

ments have also continued to improve, therefore it is necessary to create awareness and also develop proper means to tackle cases of misapplication of technology.

There are many uses for artificial intelligence, remarkable impacts have been recorded in several industries, traceable to the introduction of artificial intelligence (AI), notable industries impacted include medicine, banking, the media, and communications. On the heels of these impactful developments, controversial reports linked to deepfake technology has been significant. Deepfakes are a kind of synthetic media that uses deep neural networks and other complex machine learning algorithms to create films, pictures, and audio recordings that look and sound very genuine. Due to the ease with which these distorted forms of media may portray people, it becomes increasingly hard to separate genuine information from falsehood.

Deepfake media can be easily made by anybody who has access to fundamental AI tools & instructions. Deepfakes present a danger to the legitimacy of news media and democratic processes since they allow bad actors to broadcast false information and influence public opinion. The use of celebrity likenesses without their permission, the possibility of exploitation and harassment, and other ethical concerns have been brought up by deepfakes in the entertainment business. Deepfake technology also raises concerns about privacy and cybersecurity, identity theft as well as fraud may occur as a result of deepfakes being used for impersonations. Legal affairs are affected, as it has become possible to alter recorded audio and video, which further casts doubt on the reliability of these forms of digital materials as evidence during court proceedings.

2. Deepfakes and Data Privacy: Navigating the Risks in the Age Of AI

Conceptual clarification

Deepfakes can be likened to fake news, which was made possible by the emergence of AI in recent years. Karnouskos (2020) points out that several movies that used deepfakes appeared on social media within the last 2 years. Recent discoveries have shown that it is now possible for anyone to make and distribute false information online as it requires only a minimal level of technical knowledge and equipment.

Caporusso (2021) points out that a deepfake can perfectly copy a person's voice and read texts aloud, alternatively, they can properly overlay a person's face on someone else's body, through a technique called face swapping. This mechanism has caused a lot of tension in the data world.

Alexandrou (2019) opined that deepfakes can be viewed as fake but convincing graphics and videos, that are produced using AI technology. This process involves the combining, replacing, merging, and covering of pictures, audio and videos. Additionally, he stated that a major issue associated with deepfakes is that anyone can come up with explicit material without permission. From his works, he also argued that deepfakes are not completely inappropriate, as the technology has been used to produce some movies that caused no harm. Technological progression coupled with huge amounts of available data has helped users of the technology to make significant advancements in terms of producing visuals and audio that are of high quality, that look so real. Despite its immense benefits, most of its use has been for damaging purposes, especially for making sexually explicit content of people, for blackmailing, and other harmful purposes. The existence of deepfakes is also eroding the validity of audio and video testimonies in the courts.

According to Whyte (2020), deepfake material possesses the capacity to provide aggressors or criminals with more materials to aid their attempts to coerce, intimidate, and blackmail people. While deepfakes should be seen as a progression rather than a tool for misinformation, the way that new skills for producing effective deepfakes, coupled with the complex nature of today's digital information landscape, is making the data world considerably more dynamic than before.

Through the massive and extensive capabilities of social media, convincing deepfakes has the abilityto perpetrate significant damage to society, by spreading false information to millions of people only in a matter of minutes. In the United States of America, according to Westerlund (2019) deepfakes have been found to pose a significant threat to the society, political system, and businesses. Entrepreneurs in the fields of cybersecurity and artificial intelligence have to contend with false news, and counterfeits. Current conditions may also be helped by legislation, corporate policies while actions, education and training, and the development of technology over deepfake identification, content authentication, as well as deepfake prevention can all help combat deepfakes, as studies have shown.

As part of the positive impacts of AI in the creation of imagery, Bates (2022) contends that deepfakes and Generative Adversarial Networks (GANs) are two examples of creative AI tools that can be used to explore new horizons in the creation and editing of audio and video for advertising. These innovative capacities can drive the process of generating adverts and editing them. Several things may be done with deepfakes such as changing age, gender, or skin tone to changing voice tones, texture and even physical looks, these innovative elements can significantly impact planning, production, editing, and targeting of commercials in a positive way.

Firstly, deepfake-building systems are easier to create than to spot, this can be attributed to the effect of Generative Adversarial

Networks (GAN), which helps to ensure that the fake images and videos can evade detection methods. According to a recent study by Tolosana et al., researchers are recently emphasizing the need to concentrate on defense systems that may identify deepfakes, since deepfakes have spread from elite computer science labs to low-cost software platforms across the globe.

In recent times, psychological warfare can be waged with deepfakes, as it is possible to make clones that are identical to the original physically, behaviorally, and mentally using specialized AI software. The danger of deepfakes, in which an individual copies the speech tone and pattern of a popular is increasing in recent times. Easy access to the internet is also significantly assisting the proliferation of deepfakes. Pantserev (2020) points out that scholars are also taking into consideration the potential use of AI to curb the spread of deepfakes, as they have also been found to cause damage to the mental health of people victimized or bullied through the use of deepfakes.

Part of the danger of the prevalence of deepfake technology is that anyone who has a form of presence online, or someone whose likeness has been photographed or videotaped, stands the risk of being exposed to deepfakes and also to being "deepfaked". This is due to the commercialization of AI-technologies. Consequently, potential victims and abusers have increased, since AI-technologies have eliminated the need for victims and perpetrators to have any form of human contact or engagement. Therefore, there is a growing demand for means to avoid and prevent this form of abuse and intimidation (Cooke, 2021).

Cross (2022) argues that the prevalence of deepfakes has contributed to the growth of romance fraud across the globe. Fraudsters engaging in romance fraud usually deceive their victims to lose their money by using deepfakes to make their identities seem real. This process guarantees the loss of huge amounts of money globally. Individuals are encouraged to apply internet searches,

especially reverse image searches, to ascertain the identity of people they meet online, as a preventive strategy. This method may help victims prevent or minimize the amount of money stolen from them. It is also certain that the criminals might adapt their techniques to exploit more gaps in technology in the future, as seen in the rapid development of AI and deepfakes, which can generate unpopular, and yet convincing images. This possibility of adaptation also indicates the need for increased efforts in preventive strategies in the near future.

It is not easy to tell altered photos and videos from the genuine; nevertheless, they seem very realistic. People have slandered others, spread false information, made-up stories about terrorism/terrorist attacks, extracted money from people, and created political damage with deepfakes. Face recognition, multimedia forensics, watermarking, & convolutional neural networks, or CNNs, are some of the ways that have been developed to identify deepfakes. To identify picture or video tampering, each approach employs machine learning, a technology from the domain of artificial intelligence. (Almalki, 2019)

As the trustworthiness of online material undergoes a sea change, experts in digital picture forensics have put forward competing theories for how to consistently identify real-world AI-generated photos. The development of new uses for deepfake technology makes it clear that dual classification of picture validity is insufficient for regulating its ethical usage.

Zwitter (2020) categorizes the misuse of AI into four levels, listed as: social engineering, hacking, misinformation/fake news, and autonomous weapon systems. We may establish or modify governance plans, policies, and actions to reduce risks and avert detrimental effects by mapping these threats in advance. There is need for increased cooperation between governments, businesses, and civil society if the misuse and malevolent usage of AI is to be dealt with.

3. Data Privacy

There is an increasing recognition that the right to privacy plays a vital role in ensuring individual right to self-expression. For example, the right to privacy allows individuals to share views anonymously in circumstances where they could be criticized for expressing their opinions, it allows whistle-blowers who give critical information to protect themselves, and it also protect journalists from unlawful government interception of information. Data privacy encompasses those practices which ensure that the data shared by information providers is only used for the purpose for which it was provided. The right to privacy is contained in article 17 of the International Covenant on Civil and Political Rights (ICCPR), which says:

a. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation.

b. Everyone has the right to the protection of the law against such interference or attacks.

In addition, data protection is a legal mechanism that ensures privacy. Data protection can also be described as a legal mechanism that guarantees secrecy. It has to do with the practices, policies, and procedures an organization implements to ensure they obey legal regulations and standards. Privacy and data protection are therefore two interrelated internet governance issues.

Data protection laws are targeted towards safeguarding the processing of individuals' information, which includes information that is related to an identifiable natural person — i.e. reference to an identification number in regard to an individual's physical, physiological, mental, economic, cultural or social identity. Data protection is one of the primary measures through which the right to privacy is given effect. Data related legislation has been adopted by several countries, and many others are in the process

of doing so. The laws also play a critical role in facilitating trade amongst states, as many data protection laws help to prevent illegal cross-border data transfers, in circumstances where the state receiving the information does not offer a sufficient level of data protection.

3.1 Data Privacy Laws and Compliance

Data governance refers to the framework, policies, processes, and standards that ensure data is managed and protected effectively within an organization. It encompasses data quality, security, privacy, compliance, and data lifecycle management. Effective data governance ensures that data is consistent and trustworthy, it also helps organizations to confront expanding data privacy regulations, while employing data analytics to help inform the decision making process, while also enhancing business operations.

Data governance laws and compliance levels vary across all countries in the world. For instance, the United States just has a complex patchwork of national, state and local privacy laws and regulations. There is no comprehensive national privacy law in the United States. Although, the US does have a number of largely sector-specific privacy and data security laws at the federal level, as well as many more privacy laws at the state (and local) level. In a ground-breaking attempt, a new deepfake law was recently passed in California, USA. Summarily, the law requires that content generated through AI should be marked.

The law has three main requirements:

1. GenAI companies must mark AI-generated or altered content invisibly
2. Users must be able to add visible markings
3. GenAI companies must offer free services to identify whether content was made or altered by them

Although the law was enacted in California, its impact is expected to be global, as the law affects content providers with at least one million monthly visitors, that are publicly accessible across all the major platforms. Significantly, the law is estimated to normalize the use of watermarks that will help to easily detect deepfakes.

This law, which is expected to take effect in January 2026, will go a long way in dealing with deepfakes, however there is also a challenge with the policy. The law provides the restriction for platforms with at least a million visitors, exempting smaller platforms which could still be used for the proliferation of deepfakes.

In Africa, comprehensive data privacy laws are not common, although there are regional legal instruments that deal with data protection including: The African Union (AU) Convention on Cyber Security and Personal Data Protection 2014, EAC Legal Framework for Cyberlaws 2008, Supplementary Act on Personal Data Protection within ECOWAS 2010, and SADC Data Protection Model Law 2013. These legal instruments are subject to domestication by individual states across the subregions, ratification by national legislatures guarantees that the states have agreed to adopt the data protection laws. A major challenge observed within the continent is delay in domestication, in addition to enforcement challenges.

4. Impact of Deepfakes on Society and Individual Privacy

One major consequence of deepfakes is that they can be used to jeopardize the reputation of individuals, brands, and corporate entities. Chesney & Citron (2019) contend that deepfakes also have the potential to weaken public trust in media and information sources, which could hold significant consequences especially for democratic societies. As such, it is important to consider how deepfakes might be used to manipulate public opinion and how to develop effective strategies to combat such activities.

First, the prevalence of deepfakes helps to facilitate Misinformation and Manipulation. Deepfakes can be used to create false content that mimics the appearance and speech of real individuals. During elections it could be used to carry out manipulation of political figures or candidates, where fabricated speeches, statements or even election results can mislead the public and influence elections. Such manipulations can undermine the core principles of democracy, which rely on informed and free choices by citizens.

Secondly, the widespread dissemination of deepfake content can lead to a decline in public trust in media and information sources. If people become skeptical of the authenticity of visual and audio content, they may question the credibility of news outlets and sources they once relied on. This erosion of trust can have far-reaching implications for the functioning of democratic societies, as informed citizens are essential for making sound decisions and holding institutions accountable.

Third, deepfakes pose policy challenges for policymakers and public office holders, as deepfakes could be used to announce a false government or retract an authentic policy of the government. Governments and regulatory bodies need to consider how to address this technological threat.

As deepfake technology continues to evolve, it is likely that new and more sophisticated forms of manipulation will emerge, making it increasingly difficult to detect and combat the use of deepfakes. As such, it is important to continue to invest in research and development to stay ahead and to ensure that societies are equipped to address emerging challenges associated with deepfakes and other emerging technologies.

5. Conclusion

This paper presents an overview of deepfakes, and their societal impact on security and privacy, highlighting the challenge of discerning real media from fake media. Furthermore, the emergence of deepfakes poses significant societal and business challenges, potentially harming individuals, and eroding media trust. This paper has also highlighted the necessity for regulations, detection, mitigation, and prevention measures against deepfake misuse.

As the technology evolves, the strategies to detect and counter deepfakes must also advance. Organizations and policymakers must consider deploying security strategies on multiple levels that combine human and technological control. Identified strategies must be flexible, and proactive in dealing with further developments in the use of deepfake technology. In addition, the need for serious international collaboration, in developing standards and regulations, to manage the use and abuse of deepfakes effectively cannot be overemphasized. Global guidelines can help harmonize efforts to prevent the misuse of AI technologies across borders.

One key purpose of this paper is to spread awareness and equip the public with knowledge to defend themselves against it. The long-term solution involves critical thinking and research, aided by technology. The paper has aimed to contribute to this solution by exploring the power of design to reveal the truth and create awareness.

Conclusively, the research findings underscore the complex characteristics of the deepfake phenomena and its consequences for people, sectors, and the broader community. To alleviate the dangers of deepfake technology and encourage a better-informed and more robust digital ecosystem, it emphasizes the critical importance of immediate, preventative actions such as legislation, technical advancement, and education. Stakeholders can protect

trust, privacy, and integrity in a digitally transformed environment by recognizing and responding to these threats.

6. Recommendations

- Regulatory Framework Development: Comprehensive frameworks addressing deepfake technology should be established through collaboration between governments and regulatory authorities. Guidelines for the production, dissemination, and identification of deepfakes, as well as the repercussions for their abuse, should be laid forth in these frameworks.

- Investment in Detection and Verification Tools: Advanced deepfake detection and verification techniques should be the focus of financial resources. Among these measures is the backing of AI-powered systems that can detect deepfakes in photos, videos, and audio formats.

- Public Awareness and Education Campaigns: The presence and potential consequences of deepfake technology should be brought to the attention of the public through awareness campaigns. The significance of thinking critically and checking information while consuming media should be emphasized in these efforts.

- Media Literacy Programs in Education: Educators should include media literacy courses in their lesson plans so that students may learn to recognize fake news and other forms of manipulation. Programs like this should make digital citizenship, source assessment, and critical thinking a priority.

- Collaboration with Tech Companies: Collaboration among governments, academics, and technology businesses is critical in fighting deepfake technology. The tech industry should push for the creation and implementation of strong systems to identify and report deepfakes on their platforms.

- Ethical Guidelines for AI Development: The appropriate application of AI technology should be the primary focus of ethical standards that AI developers should follow. As part of this effort, we must encourage AI algorithm openness and include capabilities into AI systems to stop the creation of dangerous deepfakes.

Combating the spread of deepfakes is not just a technological problem, the responsibility of preserving trust in digital communication is a task for human society. The cooperation of legislators, educators, technologists and the public are important to develop strategies to address this constantly evolving threat.

Works Cited

Albahar, Mohammed, and Jameela Almalki. "Deepfakes: Threats and Countermeasures Systematic Review."Journal of Theoretical and Applied Information Technology, vol. 97, no. 22, 2019, pp. 3242–3250.

Bates, Kristyn, et al. "How Deepfakes and Artificial Intelligence Could Reshape the Advertising Industry: The Coming Reality of AI Fakes and Their Potential Impact on Consumer Behavior."Journal of Advertising Research, vol. 62, no. 3, 2022, pp. 241–251.

Caporusso, Nicola. "Deepfakes for the Good: A Beneficial Application of Contentious Artificial Intelligence Technology."Advances in Artificial Intelligence, Software and Systems Engineering: Proceedings of the AHFE 2020 Virtual Conferences on Software and Systems Engineering, and Artificial Intelligence and Social Computing, July 16-20, 2020, USA, edited by Tareq Ahram and Redha Taiar, Springer International Publishing, 2020, pp. 235–241.

Chesney, Robert, and Danielle Citron. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security."California Law Review, vol. 107, 2019, pp. 1779–1783.

Hancock, Jeffrey T., and Jeremy N. Bailenson. "The Social Impact of Deepfakes."Cyberpsychology, Behavior and Social Networking, vol. 24, no. 3, 2021, pp. 149–152.

International Covenant on Civil and Political Rights. Office of the High Commissioner for Human Rights,www.ohchr.org/en/instruments-

mechanisms/instruments/international-covenant-civil-and-political-rights.

Kapoor, Priya. "Study on the Impact of Artificial Intelligence Enabled Deepfake Technology."International Journal of Creative Research Thoughts, vol. 12, no. 5, 2024, pp. 71–101.

Karnouskos, Stamatis. "Artificial Intelligence in Digital Media: The Era of Deepfakes."IEEE Transactions on Technology and Society, vol. 1, no. 3, 2020, pp. 138–147.

Mahashreshty, Vishweshwar, and Shalini. "Implications of Deepfake Technology on Individual Privacy and Security."Culminating Projects in Information Assurance, no. 142, 2023.

Maras, Marie-Helen, and Alex Alexandrou. "Determining Authenticity of Video Evidence in the Age of Artificial Intelligence and in the Wake of Deepfake Videos."The International Journal of Evidence & Proof, vol. 23, no. 3, 2019, pp. 255–262.

Media Defence. "Litigating Digital Rights and Freedom of Expression Online: Data Protection and Data Privacy."Media Defence,www.mediadefence.org/resource-hub/privacy-security-and-data-protection/.

Westerlund, Mika. "The Emergence of Deepfake Technology: A Review."Technology Innovation Management Review, vol. 9, 2019, pp. 39–47.

Whyte, Christopher. "Deepfake News: AI-Enabled Disinformation as a Multi-Level Public Policy Challenge."Journal of Cyber Policy, vol. 5, no. 2, 2020, pp. 199–217.

Striking a Balance: Harmonizing Data Minimization and Business Objectives

Eso Ayoola, Ayodele Ayomide, Onyiriagwu Ifunanya, Nwokoye Grace and Ovie-Whiskey Victor
Lagos State University of Science and Technology
3Consulting Ltd

Abstract

Organizations are confronted with the critical task of balancing data minimization against key business objectives. Central to global privacy regulations, including the Nigeria's Data Protection (NDPAct), the principle of data minimization demands that only personal data essential for specified, explicit and legitimate purposes be collected. Yet, this principle often conflicts with business practices that rely on comprehensive data for analytics, innovation, and enhanced customer engagement. This article delves into the delicate balance between data minimization and business needs, particularly within the context of the NDP Act. It analyzes relevant regulatory frameworks, addresses the challenges faced by businesses, and explores effective strategies such as Privacy by Design (PbD) and Privacy-Enhancing Technologies (PETs) to harmonize compliance with business expansion. Using secondary data demonstrates that ethical data handling can substantially lower regulatory risks, build consumer trust, and enhance overall operational efficiency. By integrating innovative strategies and prioritizing privacy in their organizational processes, businesses can

secure a competitive advantage while fulfilling rigorous data protection mandates. This careful balance not only ensures compliance but also preserves opportunities for innovation and deeper customer engagement.

Keywords: Data Minimization, Privacy Regulations, Business Compliance, Privacy-Enhancing Technologies, Ethical Data Practices

1. Introduction

As organizations increasingly rely on data to drive customer insights, enhance operational efficiency, and maintain competitive advantage, they face the complex challenge of balancing data minimization with business needs. Data minimization, is a fundamental principle embedded in key data protection regulations, including the General Data Protection Regulation (GDPR) in the European Union and Nigeria's Data Protection Act (NDP Act), and it is a core tenet of privacy legislation globally. It requires organizations to limit data collection to what is strictly necessary for specific, legitimate purposes (GDPR, Art. 5(1)(c); NDP Act, 2023, S24). This principle supports individual privacy and mitigates risks associated with data breaches and unauthorized access. While data minimization safeguards privacy rights, it often conflicts with business objectives, where broader data access can enhance decision-making, customer experiences, and product development. Achieving an effective balance between regulatory compliance and operational needs requires a strategic approach that upholds privacy standards without hindering innovation and business growth.

The NDP Act emphasizes the importance of data minimization by mandating that data controllers and processors collect only the personal data necessary for intended purposes. This legal frame-

work compels organizations to critically evaluate their data practices, aligning them with both regulatory requirements and business goals. It constitutes a substantial advancement in the protection of individual privacy rights in Nigeria. This notion is crucial for safeguarding individual privacy, although it may occasionally conflict with the data-centric techniques utilised by organisations. This article examines the intricate equilibrium between data minimisation and business objectives under the act, highlighting the obstacles, opportunities, and best practices.

Non-compliance can result in severe penalties and reputational harm. Balancing data minimization with legitimate business needs presents unique challenges for compliance officers and business leaders. While data minimization reduces privacy risks (Information Commissioner's Office, 2019), many businesses depend on extensive data analytics for growth and competitiveness (Cavoukian, 2011). Striking this balance is essential not only for regulatory compliance but also for building and maintaining consumer trust in an era of heightened data privacy concerns. In this regard, the ongoing conflict between the need for data minimization and business requirements, analyzing how organizations can implement effective strategies to achieve compliance without compromising their operational capabilities is important. Through a review of current regulations, best practices, and industry examples, this analysis will provide insights into how businesses can responsibly navigate data minimization to remain competitive while protecting individuals' privacy.

The concept of data minimisation, as articulated in rules such as the GDPR and NDP Act, require enterprises to navigate a complex balancing act. Although these restrictions are crucial for safeguarding individual privacy, they may also impede innovation and competition, requiring a judicious approach to data gathering and processing. The convergence of data minimisation and business innovation constitutes a complex and dynamic domain. Although data minimisation guidelines are essential for protecting privacy,

enterprises must devise new strategies to reconcile these principles with the necessity for data-driven insights to maintain competitiveness. The conflict between data minimisation and company innovation prompts the inquiry of a potential trade-off between privacy and advancement, as well as, the difficulties and prospects of achieving equilibrium among these conflicting interests in the digital era.

2. Literature Review

Data minimisation is a principle grounded in social science theories that emphasise humanautonomy, privacy, and social fairness. Below are few fundamental social science theories that support data minimisation:

Theories of Privacy - The Right to Privacy by Warren and Brandeis (1890) asserts that individuals possess the right to solitude and to regulate their personal information. Data minimisation adheres to this idea by restricting the acquisition and keeping of personal information.

Westin's Privacy Framework: Westin's (1967) approach delineates five privacy rights: personal privacy, residential privacy, communicative privacy, informational privacy, and privacy of choice. Data minimisation upholds these rights by restricting the acquisition and utilisation of personal data.

Theory of Social Contract - Implicit Agreement: Social contract theory posits that individuals tacitly consent to specific laws and norms in return for the advantages of societal existence (Hobbes 1985). Data minimisation represents a societal consensus to restrict the collection and utilisation of personal information in return for the advantages of technology progress.

Ethical Theories - Deontological Ethics: This ethical framework prioritises responsibility and obligation. Data minimisation is regarded as an ethical obligation to safeguard personal privacy and

prevent unwarranted harm. Utilitarianism emphasises the maximisation of collective happiness and the minimisation of suffering. By constraining the acquisition and utilisation of personal data, organisations can mitigate possible harm and enhance overall well-being (Kant 1992).

Theories of Power and Surveillance - Surveillance Capitalism: This concept emphasises the power relations between individuals and corporations, wherein personal data is amassed and scrutinised to derive profit (Foucault 1975). Data minimisation can alleviate the power disparities intrinsic to these relationships.

Data minimization has emerged as a fundamental principle in contemporary data privacy regulations across the globe, notably within the General Data Protection Regulation (GDPR) in the EU and Nigeria's Data Protection Act (NDP Act). These frameworks unequivocally require that the collection of personal data be confined to what is essential for legitimate purposes (GDPR, 2018; NDP Act, 2023). Article 5(1)(c) of the GDPR and Section 24 of the NDP Act are designed to mitigate the risks associated with data breaches, misuse, and unauthorized access, ultimately safeguarding individual privacy rights. Gellert (2016) emphasizes that the intent behind data minimization is not just regulatory compliance; it also acts as a vital barrier against the unchecked accumulation of data and its potential misappropriation.

Furthermore, it places a clear obligation on organizations to demonstrate the necessity of each piece of personal data they collect. With global data privacy concerns escalating, authorities such as the European Data Protection Board (EDPB) have highlighted that data minimization is crucial not only for protecting personal privacy but also for fostering public trust in data-driven systems (EDPB, 2019). While data minimization is crucial for safeguarding privacy, businesses frequently depend on extensive data sets to drive growth, enhance customer experiences, and secure competitive advantages. The effective use of data is key in personalizing services, predicting customer behavior, and developing targeted

marketing campaigns. Davenport and Bean (2018) underscore the importance of data analytics as a vital business enabler, arguing that a wider, data collection, yields insights that enhance market relevance and operational efficiency. For instance, studies illustrate that leveraging customer data allows companies to accurately forecast demand, optimize supply chains, and improve customer engagement (Henke et al., 2016). However, as Stalla-Bourdillon et al. (2017) highlighted, businesses often face significant regulatory challenges when attempting to balance their data ambitions with privacy obligations, as expansive data collection practices may conflict with the principles of data minimization.

The conflict between data minimization and business objectives presents a distinct challenge for organizations trying to maintain competitiveness while complying with privacy regulations. Martin and Murphy (2017) highlight that restricting data collection can stifle innovation, particularly in industries like marketing, finance, and healthcare, where data analytics are fundamental to operations. Research by Tene and Polonetsky (2013)reveals that companies often encounter pressure to gather more data than is strictly necessary, driven by the uncertainty of future requirements. Consequently, many organizations find themselves at a critical intersection, where commitment to data minimization principles appears to clash with their strategic ambitions and the pursuit of maximizing the inherent value of data. Achieving a balance between compliance and business needs necessitates a strategic approach that weaves data protection principles into the fabric of an organization's operations. Privacy by Design (PbD), a framework established by Cavoukian (2011), serves as a solid foundation for this balance by incorporating privacy considerations at every stage of the data processing lifecycle. PbD promotes proactive privacy measures, such as data minimization, which do not obstruct business activities. By embracing PbD, companies can create systems that emphasize privacy while still gathering the data essential for Specific and legitimate business objectives. Fur-

thermore, Schwartz and Solove (2014) advocate for a risk-based approach to data management, where organizations classify data according to its sensitivity and necessity. This method not only enables organizations to retain vital data that supports business functions but also ensures a reduction in data that poses potential privacy risks. Various industries have successfully adopted practices that allow for data minimization while maintaining the flexibility required for data analytics.

The financial services sector, for instance, has effectively utilized data minimization to manage regulatory compliance and mitigate data security risks. According to Costa and Spagnoletti (2018), financial institutions often implement data minimization by developing specific, limited-purpose data sets for risk assessments and fraud detection. This approach enables them to comply with privacy regulations without sacrificing essential operational functions. In the healthcare sector, which is also heavily reliant on data, data minimization is achieved through the segmentation and anonymization of data, thus supporting medical research while adhering to privacy standards like the Health Insurance Portability and Accountability Act (HIPAA) in the United States. Research by Rumbold and Pierscionek (2017) indicates that healthcare providers are increasingly adopting anonymization techniques to ensure data minimization, facilitating research efforts without infringing on patient privacy.

Data governance structures are crucial for achieving data minimization while still aligning with business objectives. Data governance encompasses the framework and policies that oversee data processing and establish accountability for data management. Otto (2011) underscores that well-defined data governance frameworks, which include clear policies, procedures, and oversight mechanisms, can promote data minimization without disrupting business operations. Furthermore, advancements in privacy-enhancing technologies (PETs) such as differential privacy, anonymization, and encryption provide additional support for data

minimization efforts. According to Gursoy et al. (2020), PETs empower organizations to perform analytics on minimized data, enabling them to derive valuable insights while maintaining privacy safeguards. By incorporating these technologies, businesses can successfully implement data minimization strategies without impeding their analytical capabilities.

Data minimization is emerging as not just a regulatory obligation but a powerful strategy for cultivating consumer trust. A report from the International Association of Privacy Professionals (IAPP, 2019) highlights that customers tend to place greater trust in companies that restrict data collection solely to what is necessary. Schwartz and Peifer (2017) argue that effectively communicating data minimization can set a brand apart and enhance customer loyalty, especially in a landscape where data privacy is a growing concern. Similarly, Kumar et al. (2018) show that businesses that prioritize and publicly commit to data privacy and minimization can reduce the reputational risks associated with data breaches. Ultimately, earning consumer trust translates into genuine business benefits, as privacy-conscious consumers often favor and reward organizations that demonstrate responsible data stewardship.

3. Analysis

To understand the intersection between data minimization principles and business needs, it is essential to analyze existing practices and their implications. This section examines current trends in data collection, ethical challenges, and consumer attitudes, drawing on real-world case studies.

3.1 The Prevalence of Over-Collection in Business Practices

Data over-collection has become a hallmark of modern business strategies, driven by the low cost of storage, the ease of gathering

data through advanced technologies, and the perception that "more data is better" (Cavey, 2023). For instance, Gartner estimates that “over 50% of collected data remains unused, categorized as dark data information gathered during business operations but never analyzed or utilized” (qtd. in Verhulst).

This phrase underscores the prevalent tendency of organisations to accumulate more data than necessary. This excessive accumulation is propelled by multiple factors:

Reduced Storage Expenses: The declining cost of storage enables enterprises to retain substantial volumes of data without incurring considerable costs.

Technological Advancements: Contemporary technologies facilitate the aggregation of data from diverse sources, including websites, applications, and IoT devices.

Belief in "More is Better": Numerous enterprises contend that accumulating additional data would enhance insights and decision-making, regardless of a defined application for the entirety of the data.

The over-collection of data results in a substantial amount of information gathered by businesses remaining unutilised, commonly termed "dark data." This not only depletes resources but also heightens the danger of data breaches and other security concerns.

Case Study: Amazon and Recommendation Systems

Amazon collects massive amounts of consumer data to power its recommendation algorithms. While this improves customer experience, studies reveal that much of the data collected like precise clickstream information remains unused, leading to operational inefficiencies and privacy concerns (Davenport & Harris, 2022).This phenomenon stems from:

Undefined Data Purposes: Companies like Marriott have faced GDPR fines for failing to define the purpose of collected data, which made them vulnerable to breaches involving unstructured, excessive data (Zurkus, 2019).

Technological Enablement:Tools like cookies, device IDs, and IP appendages enable companies like Facebook to accumulate vast amounts of data. This indiscriminate collection contributed to the Cambridge Analytica scandal, which exploited user data for unauthorized political profiling (Erin, 2022).

3.2 Ethical and Regulatory Concerns - Over-collection poses significant ethical and regulatory risks.

Ethical Violations: Practices such as data hoarding, invasive personalization, and hyper-targeted advertising compromise consumer trust. For example, Big Tech platforms like Google and Facebook have been criticized for exploiting user data without adequate consent, culminating in legal actions and scandals like Cambridge Analytica (Erin, 2022).

Regulatory Non-Compliance: The GDPR explicitly mandates data minimization, requiring companies to justify every data point collected. Failure to comply has led to fines and reputational damage, as seen with Google Analytics, being deemed non-compliant in multiple jurisdictions (Zurkus, 2018).

Data Hoarding: Enterprises may accumulate substantial volumes of data lacking a defined purpose or retention policy.

Invasive Personalisation: The utilisation of personal data to provide highly tailored experiences can infringe upon privacy and undermine trust.

Hyper-Targeted Advertising: Overzealous surveillance and profiling may result in obtrusive and manipulative advertisements.

Regulatory Noncompliance: Security and Breach Notification: Enterprises must have stringent security protocols to safeguard personal information and inform individuals in the event of a data breach. Noncompliance with these standards may lead to substantial penalties, reputational harm, and erosion of customer confidence.

Case Study: British Airways GDPR Fine

In 2018, British Airways was fined £20 million under GDPR for failing to protect user data adequately. The breach exposed personal data of 400,000 customers, including credit card details, which were unnecessarily retained beyond their use (Information Commissioner's Office, 2020).

3.3 Impact on Consumer Trust and Loyalty - Consumer attitudes toward privacy reinforce the importance of ethical data practices.

Privacy as a Competitive Advantage: Surveys reveal that 89% of consumers prioritize privacy, and 41% in Europe distrust companies' ability to handle their data responsibly (Erin, 2022). This sentiment has driven the success of privacy-centric brands like Signal and ProtonMail.

Distrust from Over-Personalization: Over 75% of consumers perceive hyper-targeted advertisements as invasive, leading to customer attrition. Ethical missteps in data usage often result in long-term damage to brand loyalty (Freedman, 2023). This assertion highlights the detrimental effect of excessive data collecting on consumer trust and loyalty.

Privacy as a Competitive Advantage: Consumers are increasingly valuing privacy, and organisations that emphasise data protection can secure a competitive edge.

Distrust from Over-Personalization: Excessive data accumulation and hyper-targeted marketing may engender consumer distrust and adverse opinions of a company. Fundamentally, enterprises that emphasise ethical data practices and uphold consumer privacy are more inclined to cultivate trust and loyalty. Conversely, entities that engage in excessive data collecting and misuse may encounter adverse repercussions, such as customer attrition and brand harm.

Case Study: Signal's Market Growth

After WhatsApp announced changes to its privacy policy in 2021, Signal experienced a 4,200% increase in downloads, demonstrating consumer preference for secure, privacy-first messaging platforms (BBC, 2021) .

3.4 Business Implications of Excessive Data Collection - Excessive data collection often leads to operational inefficiencies and heightened risks:

Operational Challenges: Organizations struggle to organize, manage, or analyze vast datasets. A survey found that 46% of companies cannot identify the location of their sensitive data, undermining their ability to comply with regulations like the GDPR (Zurkus, 2018).

Cybersecurity Vulnerabilities: Retaining unnecessary data increases the attack surface for breaches, with over 130,000 data breaches reported in 2021 alone (Robicquet, 2022). This statement delineates the adverse commercial ramifications of extensive data collection:

Operational Difficulties: Data Overload: Enterprises may encounter difficulties in managing and analysing extensive datasets, resulting in inefficiency.

Risks of Non-Compliance: Excessive data collecting might hinder compliance with data protection requirements, as organisations may struggle to identify and safeguard sensitive information.

Cybersecurity Weaknesses: Expanded Attack Surface: Retaining superfluous data amplifies the potential for cyberattacks and data breaches.

Increased Risk of Data Loss: A greater volume of data heightens the likelihood of inadvertent data loss or unauthorised access.

Case Study: Marriott Data Breach

Marriott's 2020 breach exposed data of over 5.2 million guests, including sensitive details such as passport numbers. A significant portion of the breached data was deemed unnecessary for ongoing operations, illustrating the risks of over-retention (ICO, 2020). However, businesses that adopt data minimization principles can reduce costs, enhance efficiency, and align with consumer expectations. For example, the use of structured and purpose-driven datasets, as recommended in privacy-enhancing technologies (PETs), enables companies to meet both compliance and operational goals (Malek, 2021).

4. Strategies For Ethical Data Use - Addressing Over-Collection Requires a Paradigm Shift Toward Intentional And Ethical Data Practices

Privacy by Design (PbD): Embedding privacy considerations into data processing workflows can ensure compliance without stifling innovation (Cavoukian, 2010). Incorporating privacy issues into the design and development of systems and procedures from the outset.

Incorporating privacy into products and services from the outset, rather than as an afterthought.

Leveraging PETs: Tools like differential privacy and anonymization allow businesses to extract valuable insights while minimizing the collection of sensitive data (Malek, 2021).

Proactive Data Management: Transitioning from reactive to proactive data strategies helps businesses focus on actionable insights rather than indiscriminate accumulation *(Jackson, 2020)*. This declaration delineates techniques for ethical data use and mitigating over-collection. Mitigating the danger of re-identification and privacy violations.

Proactive Data Administration: Adopting a proactive strategy for data management instead of responding to data breaches or regulatory compliance challenges. Consistently evaluating and analysing data requirements, and eliminating superfluous data.

Establishing data retention policies to guarantee that data is retained just for the requisite duration.

5. Conclusion

The findings affirm that companies often collect more data than they need. This practice is largely fueled by the assumption that having more data offers a competitive advantage, combined with the low cost of storage and the ease of collection enabled by advanced tracking technologies. However, much of this data classified as "dark data" remains unused, highlighting a lack of clear objectives in data collection strategies. Companies do not need to gather such excessive amounts of data. Over-collection leads to significant ethical, regulatory, and operational challenges, including compromised consumer trust, inefficiencies, and heightened cybersecurity risks. Businesses benefit more from collecting and managing purpose-driven, actionable data that aligns with specific goals. By adopting data minimization principles and leveraging privacy-enhancing technologies, organizations can collect only what is necessary, ensuring compliance, fostering consumer trust,

and streamlining operations. Ethical and intentional data practices are not only a regulatory requirement but also a strategic imperative for sustainable business growth. The analysis underscores the critical importance of data minimization in today's data-driven landscape. Excessive data collection poses significant ethical and regulatory risks, including privacy breaches, consumer distrust, and operational inefficiencies. To mitigate these risks, organizations must embrace a proactive approach to data management, prioritizing privacy by design and implementing robust data governance practices.

6. Future Research Directions:

1. Empirical Studies: Conduct empirical studies to assess the effectiveness of data minimization practices in Nigerian organizations.
2. Comparative Analysis: Compare the implementation of data minimization principles in Nigeria with other jurisdictions, such as the EU and Canada.
3. Emerging Technologies: Explore the implications of emerging technologies, such as artificial intelligence and the Internet of Things, on data minimization and privacy.

The use of privacy-enhancing technologies and in following data minimisation principles, organisations can comply with legislation, build customer trust, and achieve a competitive advantage. As the legal environment evolves, organisations must stay aware and adjust their data policies to maintain compliance and ethical data management.

Works Cited

Cavey, Stephen. *"How Much Data Do You Really Need?"https://digitalisationworld.com/blog/57342/how-much-data-do-you-really-need*Accessed 10 Oct. 2024.

Cavoukian, Ann. *Privacy by Design: The 7 Foundational Principles*. Information and Privacy Commissioner of Ontario, 2011.

Costa, C., and P. Spagnoletti. *"Data Minimization in the Financial Sector." Journal of Business Research, 2018.*

Davenport, Thomas H., and Randy Bean. *Competing on Analytics: How Companies Use Data to Create Value*. Lancaster University Ghana, 2018.

Davenport, Thomas H., and Jeanne G. Harris. *Competing on Analytics: The New Science of Winning*. Harvard Business Review Press, 2006.

European Data Protection Board (EDPB). *Guidelines on Data Minimization*. 2019.

Erin. *"Privacy in Business: What Is It and Why Is It Important?"*www.matomo.org/blog/2022/07/privacy-in-business/ Accessed 6 Oct. 2024.

Foucault, Michel. *Surveiller et punir: Naissance de la prison (in French). Paris: Gallimard,* 1975.

Freedman, Max. *"How Businesses Are Collecting Data (And What They're Doing with It)." Business News Daily, 2023.*

Gellert, Raphael. *"Understanding Data Minimization: Perspectives from European Privacy Law." Computer Law & Security Review, 2016.*

Gursoy, Mehmet Emre, et al. *"Privacy-Preserving Technologies in Data Minimization." IEEE Access, 2020.*

Guyer, Paul, and Wood, Allen W. *The Cambridge Edition of the Works of Immanuel Kant in English Translation*, 16 vols., ed. Cambridge: Cambridge University Press, 1992.

Henke, Nikolaus, et al. *"The Role of Data in Modern Business." McKinsey Quarterly, 2016.*

Hobbes, Thomas. *Leviathan*. London: Penguin Books, 1985.

Information Commissioner's Office (ICO). *"Data Minimisation: A Key Principle of Data Protection." 2019.*

Information Commissioner's Office (ICO). *Marriott International GDPR Fine Report*.

2020.

International Association of Privacy Professionals (IAPP). *Data Privacy in Customer Trust*. 2019.

Jackson, Jarret. *"Businesses Have More Data Than Ever Before, But Do They Measure What They Manage?" Forbes, 2020.*

Kumar, V., et al. *"Building Trust through Data Minimization." Journal of Consumer Marketing, 2018.*

Malek, Md. Abdul. *"Bigger Is Always Not Better, Less Is More, Sometimes: The Concept of Data Minimization in the Context of Big Data." ResearchGate, 2021.*

Martin, Kirsten, and James Murphy. *"The Challenge of Balancing Data-Driven Growth and Data Privacy." 2017.*

Otto, Boris. *"The Importance of Data Governance for Compliance and Competitive Advantage." Journal of Information Technology Management, 2011.*

Pallardy, Carrie. *"How Much Data Is Too Much for Organizations to Derive Value?" InformationWeek, 2024.*

Robicquet, Alexandre. *"Why Businesses Don't Need More Data—They Need Better Data." Forbes, 2022.*

Rumbold, John M., and Beata K. Pierscionek. *"Ethical Data Practices in Healthcare." 2017.*

Schwartz, Paul M., and Daniel J. Solove. *"The Risk-Based Approach to Data Protection." 2014.*

Verhulst, Stefaan. *"Companies Collect a Lot of Data, But How Much Do They Actually Use?" The Living Library, 2019.*

Warren, S., and Brandeis l . *"The Right to Privacy". Harvard Law Review. **IV** .* Accessed 4 October 2024 – via Internet Archive.

Westin, A. Privacy and Freedom. New York, Atheneum, 1967.

Zurkus, Kacy. *"Businesses Are Collecting More Data Than They Need." Infosecurity Magazine, 2018.*

Cross-Border Data Transfers: Compliance Challenges and Best Practices for Prevention of Data Breaches

Damilola M. Adeniyi
Legal Practitioner&
Oluwakamiye T. Olorunfemi
Legal Practitioner

ABSTRACT

Cross-border data transfer is essential to the proper functioning of an international economy. Daily, people continue to make transactions and subscribe to digital platforms to access the digital tools provided by these platforms. In the process of carrying out these transactions, personal data is required and supplied. These personal data could be transferred across jurisdictions and susceptible to breach where adequate protections are not provided. This article explores the compliance challenges in managing cross-border data transfers. It also provides actionable practices for preventing data breaches, helping organizations establish a robust data protection framework that not only meets legal requirements but also protects data subjects and fosters their trust in the organization or company. In this age, data privacy and protection are paramount, and it is important for businesses to be proactive in their approach to cross-border data security to safeguard both their reputation and the data of their customers.

Keywords: Cross-border, data transfer, data breaches, compliance, legal frameworks.

1. Introduction

The advent of information and communication technology (ICT) has increasingly digitalized and globalized the world (Casalini & Gonzalez 8). Since the digitalization of the world, business operations and product manufacturing have become heavily dependent on obtaining, processing, and storing data, most especially across borders. Cross-border data transfers are integral to the daily operations of various sectors because they boost the global economy and allow businesses and consumers access to the best technologies and services wherever they may be located around the world (Hunton & Williams LLP 3).

Cross-border data transfer is the transfer of data from one country to another. Transfers are essential in aiding the transfer of data in companies and organizations, which in turn increases efficiency and the quality of the organization. The General Data Protection Regulation (GDPR) defines cross-border data transfer as the "processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to affect data subjects in more than one Member State substantially.

An individual who can be identified as the owner of a particular data is known as a Data Subject. In contrast, a person, private entity or public authority, whether natural or legal, who makes use of the personal data is known as the data processor or data controller. In Nigeria, the Nigerian Data Protection Act 2023 governs the transfer of personal data, while for countries under the European Union, the General Data Protection Regulation governs the transfer of personal data. These regulations protect an individual's

fundamental right, especially as it relates to the transfer of personal data.

2. Types of Data

Data can be transmitted through means such as email, file transfer, and cloud storage services, among many others. Various types of data exist, including personal data, financial data, and sensitive data.

According to the General Data Protection Regulation, otherwise known as GDPR, Personal data is "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"; *(Article 4, General Data Protection Regulation).*

Under personal data, there exist the following types of data, and it encapsulates these other types of data as they relate to a natural person.

i. Data concerning health, which is data related to a natural person's health, whether physical or mental and also encapsulates the provision of health information about such an individual.

ii. Biometric data, which confirms a person's physical and psychological features, helps to create a distinctive and unique identification of that person.

iii. Sensitive personal data is data that the controller must not use or permit the processor to use unless with the express consent of the data subject or in some other circumstances. If the data subject withdraws consent, the control-

ler ceases to have the right to use it. *(Section 30, Nigerian Data Protection Act 2023).*

3. Relevant Stakeholders And Their Role In Data Transfers

Data Subjects: The Data Subject is the person the personal data is about. The data subject has various rights under the laws of different countries. Generally, some rights of the data subject include the right to data portability, the right to restriction of data processing, the right to be informed about data processing, the right of access to personal data, and the right to erasure, among several others (European Data Protection Supervisor). These rights seek to protect the data of the data subject and give the subject unrestricted access within the bounds of law to its data.

Data Controllers: The Data Protection Commission defines a data controller as a person, either natural, artificial, or even a public authority, who is in charge of decision-making regarding the processing of personal data and also determines the purpose and way such personal data should be collected, stored, used, and processed (Data Protection Commission, Ireland). Furthermore, there may be instances where two or more persons or authorities are in control of personal data and for that purpose, they are called joint data controllers. The Data controller bears the liability for the particular data it controls.

Data Processors: The Data processor is a person, either a natural or artificial person, who carries out the instructions of the data controller in processing the personal data received from the data controller. The Data Processor only processes data in line with the instructions of the data controller (Article 29, UK GDPR). Whenever the data processor acts beyond the powers and instructions of the data controller, the data processor automatically becomes the controller for that personal data by also bearing the liability for

the use of the data as if it were the controller (Information Commissioner's Office, United Kingdom).

Data Protection Officers: The crucial role of the data protection officer, otherwise known as DPO, is to ensure that the use of the data subject's data complies with laws and regulations. The DPO reviews rules and regulations and offers advice to the data controller, processor, and data subject on data protection rules (Information Commissioner's Office, United Kingdom). The data controller is required by law to assign a data protection officer to work closely with the data processor in the usage of personal data. Due to the important role of data protection officers, it is advised that such persons have a high level of experience in data privacy and protection, adequate legal knowledge, and also independence in advising on risks of data transfer.

Government Agencies: These are agencies across borders that regulate the collection, processing, and transfer of personal data. In Nigeria, the Nigeria Data Protection Commission is the body responsible for regulating data protection while the General Data Protection Regulation regulates the collection and processing of personal data in the European Union. These agencies ensure that the personal data of data subjects is not compromised and is used appropriately for the right purpose.

Third-Party Service Providers: These are organizations that provide tools for data transfer, usage and processing.

4. Legal and Regulatory Frameworks Governing Cross-Border Data Transfers

As data is increasingly becoming the new economic driver in our digitalized world, protecting it during cross–border transfers is also becoming important. Data is vulnerable to mishandling during cross-border data transfer. Thus, to ensure that organizations process and transfer data across borders with transparency and

due care, many jurisdictions have established strict regulations to safeguard the handling of personal data and mitigate risks associated with cross-border data transfers. Some of these regulatory frameworks are the European General Data Protection Regulation, the Califonia Consumer Privacy Act, the Canadian Personal Information Protection and Electronic Documents Act, the Lei Geral de Protecao de Dados (LGPD) of Brazil, China's Personal Information Protection Law, and the Nigerian Data Protection Regulation, replaced by the Nigeria Data Protection Act. These regulatory frameworks make provision for the protection of data. In this section, particular reference will be made to the European General Data Protection Regulation and the Nigerian Data Protection Act.

a. European General Data Protection Regulation.

The European General Data Protection Regulation is considered one of the most comprehensive data protection regulations worldwide. Coming into force on 29 May 2018, the regulation applies to countries within the European Union and the European Economic Area. Because of the prevalence of international trade, the transfer of Personal data to countries outside the European Economic Area is inevitable. Chapter 5 of the European Union General Data Protection Regulation makes provisions for the conditions an organization has to follow to transfer data out of the European Economic Area.

Article 44 of the EU GDPR mandates that any transfer of personal data from the EU must meet strict conditions to ensure the same level of protection as within the European Union. The essence of this provision is to ensure that the level of protection of natural persons guaranteed by the EU GDPR is not undermined. Under the EU GDPR, two main bases allow personal data transfer to third countries or international organizations. The transfer may take place based on an adequacy decision under Article 45 of the EU GDPR. This implies that the Commission must have decided that

the third country or the organization receiving the data has ensured an adequate level of protection. Additionally, while assessing the level of protection, the Commission considers elements like the rule of law, respect for human rights, fundamental freedom and whether or not the rights of data subjects are effective and enforceable in the country, whether there is a functioning independent data protection authority in the third country and the international commitments the country or the organization has entered into. The European Union Commission publishes a list of the countries for which it has decided that an adequate level of protection is no longer ensured.

In the absence of an adequacy decision by the European Commission, Article 46 of the EU GDPR makes provision for a data controller or processor to transfer personal data to a third country provided that appropriate safeguards have been ensured by the data controller/processor or on the basis that they have made available for the data subjects enforceability of their rights and effective legal remedies. Consequently, there are a series of transfer tools containing "appropriate safeguards" that may be used to transfer personal data to a third country in the absence of adequacy decisions such as Standard Contractual Clauses, Binding Corporate Rules, Code of conduct, Certification Mechanisms, and Ad hoc Contractual Clauses.

Standard Contractual Clauses (Article 46 (2) (b) (c), EU GDPR) are pre-approved model contracts by the EU Commission that help to ensure that data is protected when transferring outside the EU. Companies that are not under the European Economic Area can incorporate SCCs into their contracts to ensure maximum protection of the data in the process of cross-border data transfer between European Union Countries and non-European Union states (European Commission). Secondly, **Binding Corporate Rules** are internal rules and policies for data transfers within multinational companies (PWC). It allows an organization with the European Union to transfer data to the same organization in a third country

that does not have an adequate level of protection, like the European Union (Article 46 (2) B and 47, EU GDPR). **The Code of Conduct** under the GDPR is a set of rules that an organization creates to assist its members with compliance with data detection and accountability in specific sectors or relating to particular processing operations (46 (2) (e), EU GDPR).

Finally, apart from adequacy decisions and appropriate safeguards, one other avenue of allowing transfers of personal data to a third country is based on derogation, subject to fulfilling the conditions listed in Article 49 of the EU GDPR. Importantly, in the transfer of data to third countries or organizations, data controllers/processors must ensure that all other requirements for the protection of personal data in the EU GDPR are complied with, meaning that they must have a legal basis for the communication of data, they must implement security measures, ensure data minimization, entering into contracts if the recipient of the personal data is a data processor. Failure to comply attracts sanctions by the EU Commission.

The European Commission has, on several occasions, imposed fines for breaches of cross-border data transfer rules in the EU GDPR. For example, in August 2024, complaints were laid against Uber Technologies for collecting sensitive data of drivers from Europe and retaining them in their server in the United States of America, where its centralized IT is located (Alvarez et al. 2). Since the Uber European headquarters is based in the Netherlands, the case was transferred to the Netherlands for adjudication. Uber argued that following the invalidation of the EU-US Privacy Shield by the European Union Court of Justice they relied on the EU-US Data Privacy Framework, Uber removed Standard Contractual Clauses (SCCs) from its data sharing agreements between EU and US entities and relied on the EU Q & A on the 2021 EU Model Contractual Clauses indicating that the controller to controller SCCs would not be appropriate in circumstances where the importing entity's processing operations are already directly subject to the

GDPR under Article 3 of the GDPR (Alvarez, et al. 2). However, the Dutch Data Protection Authority rejected this position and held that it was inconsistent with the provisions of the GDPR, and imposed a fine of the sum of £290 Million for the violation of the GDPR. This decision reiterates the fact that strict compliance with the provision of Chapter 5 of the EU GDPR is paramount, and entities must ensure that when personal data is being transferred from its EU entity to its counterpart in a non-EU, the appropriate safeguards are employed.

b. The Nigeria Data Protection Act 2023

The Nigeria Data Protection Act (NDP Act) is the successor to the Nigeria Data Protection Regulation, which is now a subsidiary legislation for safeguarding and processing Nigerians' personal data both at home and abroad. The Nigeria Data Protection Regulation states that data must be processed for a specific, legitimate, and lawful purpose consented to by the Data Subject (DLA Piper, Nigeria). The Nigeria Data Protection Act provides a legal framework for the protection of personal information, and it also establishes the Nigeria Data Protection Commission to serve as the body regulating the processing of personal information in Nigeria.

Part VIII, particularly Sections 41-43 of the Nigeria Data Protection Act, establishes guidelines for cross-border data transfers (Kalu & Kekema 4). Section 41 of the NDP Act restricts the transfer or permission of the transfer of data by a data processor or data controller from Nigeria to another country unless the recipient of the personal data is subject to a law, binding corporate rules, contractual clauses, code of conduct, or certification mechanism that affords an adequate level of protection concerning the personal data by the Nigeria Data Protection Act (NDP Act). This provision is similar to the provision of Section 46 of the EU GDPR which makes provisions for the employment of appropriate safeguards in cross-border data transfer. Section 42 of the NDP Act makes pro-

visions for the criteria that would be considered by the Nigeria Data Protection Commission in assessing the adequacy of protection, which includes the availability and enforceability of data subject rights and redress mechanisms, the existence of agreements ensuring data protection between the relevant authorities, public authority access to personal data, effective data protection laws and functioning of independent supervisory authorities with enforcement powers. International commitments and memberships in regional or multilateral organizations are also assessed.

Finally, Section 43 of the NDP Act further provides for instances where personal data transfers are permitted even though the requirements for transfer under Section 42 of the Act have not been met. Hence, transfers may occur if the data subject consents despite knowing the risks and has not withdrawn it; where it is contractually necessary, where it would benefit the data subject; where the transfer is crucial in the interest of the public, it would be allowed; where the transfer is necessary to defend a legal claim, and where the transfer would protect the vital interests of the data subject or others when the data subject cannot give consent.

5. Compliance Challenges In Cross-Border Data Transfers

There is a plethora of challenges that influence compliance with regulations in cross-border data transfers. Below are a few challenges that are spread across different sectors and affect the stakeholders in cross-border data transfers.

Jurisdictional Conflict: The existence of various laws regulating different jurisdictions can cause a conflict of laws in the event of a cross-border transfer. According to the Organization for Economic Cooperation and Development (OECD), jurisdictional conflict was the most cited challenge in cross-border data transfer. It was ad-

vised that significant revisions to the existing laws are needed to ensure suitability to the dynamics of the digital market. Countries that have not enacted data protection laws can consult with other existing regulations to lessen conflicts associated with the various jurisdictional laws (Idris, Adeniran. 6-7)

Technical Problems: Although the data controller and other stakeholders may take measures to ensure the smooth transfer of data from one border to the other, there is still a risk of technical problems, such as data loss, programming errors, software or hardware errors, hacking, data corruption or even wrong data access requests made to data service providers which may cause inaccuracies in data transfer (Smriti, and Jha. 9). In the event of this issue, complying with the regulations in place for data transfer may be challenging for the organization.

Security Risks: Data security risks can severely impact an organization, which is why companies must take the utmost precautions to follow the laws and regulations in place during cross-border data transfer.

Obtaining Requisite Consent And Permits: Given the critical importance of data, it is necessary to obtain both the data subject's consent and approval from the relevant regulatory authority in the jurisdiction. Without consent, data processing or transfer becomes unlawful, and if consent is withdrawn, the data processor must halt the transfer and processing immediately. Similarly, some personal data may require regulatory permits before it can be legally processed. Failure to secure these permits can result in severe penalties for the organization. Acquiring these permits can be challenging, depending on the specific laws and the regulatory agency involved, and organizations must not rely solely on back-end processes for data transfers.

Regulatory Complexities: Since laws and legislative drafting are mostly complex for non-lawyers to understand, it creates complexities in understanding the legal texts by organizations and

companies. Studies have shown that organizations may lack awareness of the provisions of the GDPR or struggle to comprehend them, organizations must ensure that there is compliance with the regulations guiding the specific data transfer (Smirnova, Travieso-Morales, 338). The Data Protection Officer is useful in this regard by offering advice on the relevant laws in that particular jurisdiction and also the host country for the data transfer while also providing innovative ideas on how to comply with the regulations.

6. Best Practices For Prevention Of Data Breaches In Cross-Border Data Transfers.

Data breaches in cross-border data transfer are on the rise these days because of the prevalence of international trade, and foreign participation in countries around the world. Hence, the prevention of data breaches in cross-border data transfer is important and can be achieved through a combination of robust technological solutions, compliance with regulatory frameworks, and organizational policies. Some key practices that can be engaged in by organizations to mitigate data breaches in cross-border data transfers are as follows:

1. **Adoption of International Data Transfer Mechanisms**: Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) and other internationally recognized frameworks for lawful data transfers are crucial tools developed by data protection authorities to promote the transfer of data across international borders without breaching data privacy rights. Businesses may guarantee a uniform degree of data protection by including SCCs in their contracts (Singh 365). On the other hand, since Binding Corporate Rules are used internally, large corporations or multinationals with many subsidiaries around the globe may benefit from employing Binding Corporate Rules in their internal regulations

(Singh 365). In the use of these tools, organizations must ensure that these tools are approved for use by the regulatory authorities of the countries the data are being transferred to or from.

2. **End-to-End Encryption of Data During Transfer and at Rest**: Encryption if data guarantees that data is kept private throughout the process of transmission, preventing unwanted access, and even if it is intercepted, it remains unintelligible without a decryption key (Singh 366). End-to-end encryption protocols like TLS/SSL can be used for data while in transit. When the data is at rest, encryption techniques like AES-256 can be used to make sure that stored data are encrypted and protected (Singh 366).

3. **Conducting Regular Data Protection Impact Assessments (DPIAs)**: A DPIA is a process that helps an organization identify and minimize the data protection risks of a project (Information Commissioner's Office 13).

4. **Setting up Comprehensive Data Processing Agreements**: in a situation where the data controller and the data processors are different entities, a Data Processing Agreement must be entered into to secure the protection of the personal data of the data subjects being used. A Data Processing Agreement is a contract between a data controller and a data processor that sets out their respective rights and obligations concerning the nature of the processing activities and the personal data being handled (Secure Privacy).

5. **Monitoring and Auditing Third-Party Vendors**: Auditing Third-party vendors is an important component of a comprehensive IT security strategy that can be employed by an organization in identifying and assessing the security practices of their vendors, ensuring that they meet the security standards required in the protection of data and also complying with regulatory requirements (Ilori, Nwosu, & Naiho 214).

6. **Staying updated with evolving regulatory requirements**: It is important to stay constantly updated on the improvements

made to existing regulatory frameworks to comply with regulatory requirements. Breaches can be avoided if organizations regularly revise data protection laws.

7. **Consulting Data Protection Experts**: Businesses and organizations can minimize data breaches by consulting legal experts in data protection or privacy consultants to assess the transfer mechanisms to be used in contracts and other contractual agreements. Employing their services can expose businesses to specific jurisdictional requirements and obligations required in cross-border data transfers.

7. Conclusion

Personal data is a crucial asset that requires stringent safeguards to prevent breaches, especially during cross-border data transfers where risks are heightened. This article has explored the challenges influencing compliance with regulatory requirements in cross-border data transfer such as conflicting laws in different jurisdictions, security risks, obtaining requisite consents and permits, and regulatory complexities amongst others. In this regard, this article further proposed key practices that may be engaged in by organizations to navigate these compliance challenges such as adopting international data transfer mechanisms, using end-to-end encryption of data to prevent breaches, conducting regular data protection impact assessments, monitoring and auditing third-party vendors where they are involved in the data transfer, and also staying updated with evolving regulatory requirements amongst others. These best practices can be adopted by data controllers and processors ensure that regardless of the jurisdictional complexities, maximum protection is afforded to personal data and by doing this, compliance will be fostered in our increasingly digitalized global world and data breaches will be minimized.

Works Cited

Ademuyiwa, Idris, and Adedeji Adeniran. Assessing Digitalization and Data Governance Issues in Africa. Centre for International Governance Innovation, 2020. JSTOR,http://www.jstor.org/stable/resrep25330. Pp 6-7 Accessed 26 Nov. 2024

Alvarez, Daniel. Jehl, Laura. Pollard, Briony. Rohol, Susan. Prochaska, Karl. "Dutch DPA Fines Uber £290m for GDPR Data Transfer Violation" Wilkie Farr & Gallagher LLP. Pp. 1-4 (2024). Web. 24 Nov 2024 <https://www.willkie.com/publications/2024/09/dutch-dpa-fines-uber-290m-for-gdpr-data-transfer-violation>

Casalini, Francesca. Lopez Gonzalez, Javier. "Trade and Cross-Border Data Flows" OECD Trade Policy Papers. No. 220 pp. 1-40. (2019). Web. 23 Nov 2024. <https://www.oecd-ilibrary.org/trade/trade-and-cross-border-data-flows_b2023a47-en>

Directorate-General for Justice and Consumers. "Standard Contractual Clauses for International Transfers (SCC)" European Union Official Website (2021). Web. 14 Nov 2024 <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en>

European Data Protection Supervisor. "Rights of the individual"European Union Official Website. Web. 29 2024<https://www.edps.europa.eu/data-protection/our-work/subjects/rights individual_en#:~:text=The%20GDPR%20has%20a%20chapter,decision%20based%20solely%20on%20automated>

Ferracane, Martina. "Restrictions on Cross-Border Data Flows: A Taxonomy" ECIPE Working Paper, No.1, (2017). Web. 16 Nov 2024 <https://ecipe.org/wp-content/uploads/2017/11/Restrictions-on-cross-border-data-flows-a-taxonomy-final1.pdf. >

Hunton, Williams LLP, "Business without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity" United States Chamber of Commerce and Huston &Williams LLP, pp. 1-43. Web. 14 Nov. 2024 <https://www.huntonak.com/media/publication/3086_Business_without_Borders.pdf>

Ilori, Oluwatosin. Nwosu, Tochi. Naiho, Henry. "Third-party vendor risks in IT Security: A Comprehensive audit review and mitigate strategies" World Journal of Advanced Research and Reviews pp. 213-224. (2024) Web. 24 Nov 2024

<https://wjarr.com/sites/default/files/WJARR-2024-1727.pdf>

Information Commissioner's Office, United Kingdom "What are controllers and processors?" Web. 28 Nov. 2024 https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and-processors/controllers-and-processors/what-are-controllers-and-processors/#1.

Information Commissioner's Office. "Accountability and Governance: Data Protection Impact Assessments (DPIAs". 1. 0. 77 pp. 1.44. (2018). Web. 25 Nov 2024 <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias-1-0.pdf. >

Kalu, Lazarus. Kekema, Temitope. "The Legal Framework for the Transfer of Personal Data of Nigerian Citizens to Foreign Countries: Exploring the Case in Suit: FHC/ABJ/CS/1246/2022 between Incorporated Trustees of Ikigai Innovation Initiative and National Information Technology Development Agency (NITDA) in the Light of the Nigeria Data Protection Act 2023." Advocaat Law Practice, pp. 1-5. (2024). Web. 20 Nov 2024 <https://advocaat-law.com/wp-content/uploads/2024/04/THE-LEGAL-FRAMEWORK-FOR-THE-TRANSFER-OF-PERSONAL-DATA-OF-NIGERIAN-CITIZENS-TO-FOREIGN-COUNTRIES-1.pdf>

Organization for Economic Co-operation and Development (OECD). "Main challenges to Cross Border Data Flows". (2019). Web. 25 Nov. 2024 <https://www.oecd.org/en/topics/sub-issues/cross-border-data flows.html#:~:text=However%2C%20cross%2Dborder%20data%20flows,security%2C%20regulatory%20reach%20and%20trade.>

Parsheera, Smriti, and Prateek Jha. "Existing Mechanisms for Cross-Border Data Access: Cross-Border Data Access for Law Enforcement: What Are India's Strategic Options?" Carnegie Endowment for International Peace JSTOR. (2020) pp. 9–14. Web. 26 N0v. 2024. <http://www.jstor.org/stable/resrep27702.6>

PwC. "Binding Corporate Rules: The General Data Protection Regulation" (2019). Pp. 1-12 Web. 23 Nov 2024 <https://www.pwc.com/m1/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf>

Secure Privacy. "Understanding GDPR Data Processing Agreements: The Definitive Guide" Secure Privacy (2024). Web. 24 Nov 2024 <https://secureprivacy.ai/blog/ultimate-guide-to-data-processing-agreements>

Singh, Anvesha. "Cross-Border Data Transfers: Legal Challenges and Solutions in

the Global Digital Economy" Indian Journal of Integrated Research in Law. Vol. IV Issue I pp. 356-368. Web. 24 Nov 2024 <https://ijirl.com/wp-content/uploads/2024/02/CROSS-BORDER-DATA-TRANSFERS-LEGAL-CHALLENGES-AND-SOLUTIONS-IN-THE-GLOBALIZED-DIGITAL-ECONOMY.pdf.>

UNCTAD. "Data Protection Regulations, and International Data Flows: Implications for Trade and Development" United Nations Conference on Trade and Development (UNCTAD) pp. 1-154 (2016). Web. 22 Nov. 2024 <https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf>

Yelena, Smirnova, Victoriano, Travieso-Morales. "Understanding Challenges of GDPR Implementation in Business Enterprises: A Systematic Literature Review" International Journal of Law and Management. Vol. 66. 3. Pp. 326-344. (2024). Web. 23 Nov 2024. <https://www.emerald.com/insight/1754-243X.htm>

Role of Data Protection Authorities in Nigeria (NDPC) and Brazil (ANPD)

Jean Carlo Jacichen Luz
IAPP Certified Information Privacy Manager (CIPM);
Certified Data Protection Officer (CDPO/BR);
Privacy Bar Section Advisory Board Member.

ABSTRACT

The article examines the crucial role of Data Protection Authorities (DPAs) in Nigeria (NDPC) and Brazil (ANPD) in enforcing comprehensive privacy laws inspired by the GDPR framework and protecting the rights of data subjects. In both countries, DPAs have been established as independent entities with responsibility for overseeing compliance with data protection laws. They have powers to investigate possible violations, impose sanctions and promote public awareness of the importance of data protection. Although they share very much similar responsibilities, there are some notable differences in their regulatory structures. The article highlights the challenges faced by the Nigerian and Brazilian DPAs and underscores the importance of international cooperation, which both recognize as crucial, particularly in the context of evolving data protection legal frameworks, increasing cross-border data flows, and emerging complex challenges such as the proliferation of AI systems. In conclusion, while the DPAs of Nigeria and Brazil each face unique challenges, their collaboration holds significant potential to align enforcement actions, facilitate the sharing of best practices, foster mutual learning, and enhance regulatory responses in the rapidly evolving, data-driven global economy.

Keywords: Data Protection, Privacy, Data Protection Authority, International Data Transfer, Compliance.

1. Introduction

In a globalized world where information and personal data are accessed simultaneously across borders, privacy and data protection have become a universal concern for people everywhere. Privacy is no longer a topic confined to discussions within restricted groups, but has become a subject of everyday conversations in society. People are increasingly concerned about their privacy and how their personal data is being collected and used by companies and governments. Not only have privacy laws proliferated worldwide, but they have also shown similarities in the essential elements of their structures.

As Danilo Doneda points out, data protection laws are showing a clear tendency to converge, as the nature of the subject matter discourages the adoption of isolated national legal solutions. The cross-border transfer of personal data, driven by global business operations and digital technologies, requires harmonized rules to ensure effective protection of individuals across different jurisdictions.

Similarly, the Centre for Information Policy Leadership (CIPL) emphasizes the need for global convergence and interoperability between privacy laws. Consequently, countries are aligning local regulations with global standards to foster legal certainty for business and ensure adequate protection for individuals in the search for balancing innovation and fundamental rights.

As outlined by the Organisation for Economic Co-Operation and Development (OECD), although national laws and policies may differ, there is a shared interest among countries in protecting priva-

cy and individual liberties. This common goal has led to the widespread adoption of robust data protection frameworks, such as the European Union's General Data Protection Regulation (GDPR), which is widely regarded as a benchmark for data protection standards.

The GDPR has not only set a high standard within the EEA countries but has also inspired similar legislative frameworks and data protection practices in numerous countries around the world. Nigeria, with its Data Protection Act (NDP Act), and Brazil, through its Data Protection Law (LGPD), are among those that have embraced a comprehensive law approach like the GDPR's.

These laws prioritize key elements such as transparency, accountability, security obligations, legal basis for data processing, and data subject rights. They also establish robust provisions regarding data breaches and cross-border data transfers, reflecting a commitment to aligning with the global movement toward stronger and more harmonized privacy rules. The similarity is noted from the structure and rationale of both legislations, which have a risk-based approach, to the different concepts provided for in the laws. A cornerstone of these frameworks is the establishment of national data protection authorities (DPAs). Conceived as independent entities, DPAs are tasked with the critical responsibility of ensuring compliance with data protection laws and in safeguarding data subject's fundamental rights.

Moreover, DPAs must be equipped with the necessary resources and expertise to perform their tasks effectively, since the continuously evolving technological landscape presents new data protection challenges every day. This requires not only sufficient financial and human resources but also access to cutting-edge tools and training to stay ahead of emerging risks and ensure robust enforcement of data protection laws. For instance, the deployment of artificial intelligence (AI) technologies across various domains around the world, which often involves the processing of

personal data on large scale, raises complex legal and ethical challenges. Although the data protection legal frameworks are similar, there are diverse approaches which combines elements from the GDPR with cultural, social and legal traditions and nuances unique to each country. These differences demonstrate the adaptability of data protection regulations to local contexts while maintaining core privacy principles in effect.

Given this context, this article aims to explore the role of data protection authorities in Nigeria and Brazil, highlighting their importance in enforcing privacy laws. Furthermore, the article explores how these DPAs, both with notable progress in the field of data protection in their respective countries, could benefit from the exchange of knowledge and experiences to improve their practices and further develop their data protection ecosystems.

2 Critical Role Of Data Protection Authorities And Enforcement Challenges

In recent years, the GDPR has had a significant influence on the formulation of data protection laws around the world. The possibility of obtaining "adequate" status with the EU, which facilitates trade and data exchange, encourages countries to adopt laws that meet GDPR requirements. DPAs play a central role in these legal frameworks, acting as key regulators in the enforcement of privacy laws and safeguarding individuals' personal data. These authorities are essential in ensuring compliance with data protection regulations, investigating potential infractions, and providing guidance to organizations on best practices. According to Graham Greenleaf, the existence of an active DPA, including collaboration between DPAs, is considered one of the most important indicators of law enforcement effectiveness.

As privacy concerns grow worldwide, DPAs are increasingly pivotal in maintaining the integrity of data protection systems across dif-

ferent jurisdictions. Having an active DPA means the authority is actively involved in supervising, investigating and enforcing data protection laws. They also have normative powers to issue regulations and guidelines that complement existing laws, clarifying legal provisions and detailing specific obligations for data controllers and processors. In practice, DPAs also fulfill the role of guiding and facilitating compliance, since some obligations require the implementation of measures that need to be calibrated according to the risk of the operations. Another relevant factor is the normative power of DPAs, which helps legislation remain up to date and relevant in the face of incessant technological development.

Furthermore, they promote public awareness of rights and responsibilities related to data protection and encourage the adoption of good practices and security standards to enhance the protection of personal data. In essence, DPAs serve as the guardians of data protection, ensuring that legislation is both effective and practical for data subjects, controllers and processors. The relevance of data protection laws and consequently of DPAs, becomes even more pronounced in the context of countries with significantly large populations, such as Nigeria, with approximately 223 million inhabitants, with over 100 million internet users, and Brazil, with roughly 216 million inhabitants. In such countries, the sheer volume of personal data being processed creates unique challenges.

The application of a data protection law must consider companies of different sizes and sectors in addition to meeting the different realities of the population itself. These complexities place additional demands on regulatory authorities, necessitating robust oversight mechanisms to ensure compliance and safeguard personal data in an effectively way. Moreover, raising awareness about data protection in populous nations can also be a significant challenge, as there are audiences with different levels of access to education and technology. Bridging this gap requires

sustained efforts, including public campaigns and educational initiatives.

It is worth noting that the data protection laws in Nigeria and Brazil are relatively recent in relation, for example, to the European tradition. In practice, this reflects the difficulty of different actors in implementing legislation in practice and ensuring compliance with the rules and protection of personal data holders. This raises the need for DPAs to take action in their guiding and regulatory role.

Technological advancements, particularly in artificial intelligence (AI), present additional challenges for DPAs. AI systems often rely heavily on the processing of personal data throughout their lifecycle, raising complex issues around risks, privacy and security. Recognizing this, the European Data Protection Board (EDPB) emphasizes the critical role DPAs should play in AI regulation. With their established expertise in data protection and their understanding of the associated risks, DPAs are well-positioned to oversee the ethical and lawful deployment of AI systems, ensuring that such technologies respect fundamental rights and adhere to robust security standards.

In this context, fostering collaboration between DPAs and various stakeholders becomes essential to effectively address these challenges. Strategic partnerships can significantly enhance outreach initiatives. By leveraging the expertise and resources of these diverse actors, DPAs can develop innovative solutions and bridge knowledge gaps.

In Africa, the African Union's Convention on Cybersecurity and Personal Data Protection, also known as the Malabo Convention, signed by Nigeria in 2024, sets a foundational standard for data protection across the continent. This landmark framework represents a significant step toward fostering a unified approach to data protection, electronic transactions, and cybersecurity within the African countries. The Convention is a comprehensive

framework of general rules and principles addressing three key themes: electronic transactions, personal data protection and promoting cybersecurity and combating cybercrimes. By encompassing these interrelated areas, the Convention aims to create a cohesive approach of secure and trustworthy digital ecosystems across its member states.

Notably, the Malabo Convention mandates that each State Party establish a national personal data protection authority. This authority must function as an independent administrative body tasked with ensuring that personal data processing complies with the provisions of the Convention. In these contexts, digitalization and expanded access to digital technologies and services generate an exponential increase in the flow of personal information, increasing the risks of breaches and other privacy-related challenges.

As noted by Dr. Vincent O. Olatunji, National Commissioner of the Nigeria Data Protection Commission, “data protection at its nascency is not without modest challenges, particularly in the area of awareness and compliance”. For instance, initiatives such as the collaboration between the ANPD and the National Consumer Secretariat (SENACON), in Brazil, demonstrate how DPAs can address these challenges. Their joint publication of the guide “How to Protect Your Personal Data” serves as an example of efforts to empower consumers by raising awareness about the importance of data protection and offering practical insights for safeguarding personal information.

Similarly, the Information Security Guide for Small Processing Agents, published by ANPD in 2021, serves as a practical tool to help smaller businesses implement data security measures effectively and be LGPD compliant.

In this landscape, DPAs plays a central and strategic role in promoting responsible data governance and in safeguarding fundamental rights in relation to the processing of personal data.

From a practical perspective, one of their primary challenges lies in providing clear and actionable guidance to help data controllers and processors comply with regulations in their day-to-day operations. Additionally, the complexity of cross-border data flows necessitates that DPAs coordinate with their international counterparts to address jurisdictional overlaps and ensure coherent enforcement. As digital ecosystems continue to expand, the strategic role of DPAs becomes increasingly critical. The issuance of adequacy decisions to enable international data transfer between countries may be one of the expected results of this joint work.

3 NDPC and ANPD Overview

The data protection legal frameworks in Nigeria and Brazil are relatively recent when compared to the European Union, which had established legislation on the subject well before the advent of the GDPR, such as the Directive 95/46/EC. Thus, it can be said that the tradition of personal data protection in Nigeria and Brazil is still in full development, acquiring its own nuances according to the particularities of these countries.

In June 2023, President Bola Ahmed Tinubu enacted the Data Protection Act of 2023 (NDP Act). Among its objectives, the Act seeks to protect the fundamental rights, freedoms, and interests of data subjects, as enshrined in the 1999 Constitution of Nigeria. The Nigeria Data Protection Commission (NDPC) , also referred to as the "Commission", was established under the NDP Act to replace the Nigeria Data Protection Bureau (NDPB). The NDPC is tasked with a broad range of responsibilities to safeguard personal data. These include regulating technological and organizational measures for data protection, fostering the development of data protection technologies aligned with international standards, and accrediting entities to provide compliance services. The NDPC also registers data controllers and processors of major importance, promotes

awareness of personal data protection, and addresses complaints related to violations of the NDP Act or its regulations. NDPC can also participate in international fora and engage with DPAs to regulate cross-border data transfers.

In turn, Brazil's National Data Protection Authority (ANPD) was established under the Brazilian Data Protection Law (LGPD) of 2018. The provisions of the LGPD became applicable on different dates. In 2018, the rules regarding the structure and functioning of the ANPD came into effect, although the authority itself was only officially established later with the appointment of its board of directors. In 2020, the majority of the law became applicable, excluding the provisions concerning the administrative sanctions, which only came into effect in 2021.

In a similar way as the NDPC, the ANPD holds the primary responsibility for safeguarding personal data and ensuring compliance with the LGPD (Article 55-J, LGPD). Among its key roles is disseminating knowledge about the LGPD, fostering public awareness of the importance of data protection, and promoting a culture of privacy within society. The ANPD also plays a role in interpreting the LGPD, providing guidance, addressing doubts, and defining the procedures for its effective application. To this end, ANPD can issue regulations and operational guidelines aimed at ensuring the security and privacy of personal data.

Some highlights of the regulations issued by the ANPD to this date are those on small processing agents, dosimetry and application of sanctions, breach notification, role of the data protection officer (DPO) and cross-border data transfers and standard contractual clauses (SCCs). In addition to its regulatory and educational functions, the ANPD is tasked with monitoring compliance and enforcing the LGPD. It can investigate cases of non-compliance and has the authority to impose a range of sanctions, such as warnings, fines, public disclosure of infraction, blocking or deletion of

data, suspension of data processing activities and ban on the execution of data-related operations.

Although both DPAs share similar overarching responsibilities, there are notable distinctions between their regulatory frameworks. For instance, the NDPC has the authority to issue directives that define additional categories of personal data as sensitive which is not possible in the context of the ANPD role, as the LGPD establishes a strict list of what are sensitive personal data, leaving no scope for expansion beyond the predefined list.

Another significant difference lies in the concept of "data controllers and data processors of major importance," a category recognized under the NDP Act's regulatory framework but absent from the LGPD. Entities falling within this classification in Nigeria are required to register with the NDPC, that shall maintain and publish on its website a register of duly registered controllers and processors of major importance.

This registration obligation is designed to enhance oversight and ensure robust data protection measures in critical sectors of the Nigerian economy, particularly for organizations handling substantial volumes of personal data or data concerning large numbers of individuals.

It is worth noting that both authorities became members of the Global Privacy Assembly (GPA) in 2023, an international forum that has united data protection and privacy authorities worldwide for over four decades. There are currently more than 130 data protection and privacy authorities accredited as members of the GPA. A country's participation in the GPA is crucial for fostering international collaboration on privacy and data protection issues. As a global forum, the GPA enables members to share best practices, develop harmonized approaches to emerging challenges, and strengthen their regulatory frameworks. Among the objectives of the GPA of 2023-2025 is the promotion of actions to exchange experiences and good practices between data protection and priva-

cy authorities that give rise to instruments and mechanisms that facilitate the enforcement of personal data protection and privacy policies.

Both the NDPC and the ANPD share the responsibility of navigating the complexities of the rapidly growing digital ecosystems. With large populations and increasing internet penetration, both Nigeria and Brazil face unique challenges in ensuring compliance across diverse sectors, which emphasizes the importance of exchanging knowledge with other data protection authorities.

4 Possible Cooperation between DPAs

The NDP Act expressly provides that the NDPC may participate in international forums and collaborate with data protection authorities with a view to developing strategies for regulating cross-border transfers of personal data (Article 5. J).

The Nigeria Data Protection Annual Report of 2023 underscores the Commission's emphasis on bilateral and multilateral cooperation. It acknowledges the inherently global interconnectedness of data processing platforms and emphasizes that safeguarding data privacy rights, ensuring national security, fostering the growth of the country's digital economy, and maintaining the nation's data sovereignty can only be effectively achieved through collaborative efforts with other data protection authorities. As stated at the annual report, the outcomes intended encompass the exchange of knowledge on data protection and privacy, fostering mutual legal assistance in investigating data breaches, supporting the enforcement of transborder decisions, and facilitating intergovernmental information sharing.

On the side of the ANPD, one of its key responsibilities is to foster cooperation with data protection authorities from other countries, as established in Article 55-J, IX of the LGPD. With this provision, the ANPD can aim to exchange expertise, harmonize approaches,

and address global data privacy issues effectively. In this regard, the ANPD has signed a memorandum of understanding with the Spanish Data Protection Authority (AEPD) for the development of joint actions to promote the disclosure and practical application of data protection regulations. One of the objectives is to promote specific technical cooperation mechanisms that allow the exchange of knowledge and experiences, in addition to identifying best practices in the field of personal data protection.

Another example is the recently signed memorandum of understanding with the Office of the Privacy Commissioner of Canada (OPC) for cooperation and mutual assistance in the field of data protection. The agreement aims to strengthen institutional relations between the two nations and encourage technical, regulatory and supervisory cooperation. This reflects the intrinsic understanding of the Nigerian and Brazilian authorities that the protection of personal data is a global challenge that requires joint efforts between countries. International cooperation allows for the sharing of experiences, the harmonization of standards, especially in regard of data flows across borders, and the creation of more effective mechanisms for protecting data privacy in an increasingly interconnected world.

Both Nigeria's NDPC and Brazil's ANPD acknowledge the critical importance of international cooperation in the field of data protection. Their participation in the Global Privacy Assembly 2023 underscores their commitment to fostering global collaboration. The shared recognition between the NDPC and ANPD of the need for international cooperation highlights the importance of adopting a unified, global approach to data protection. Such collaboration between DPAs is essential to ensure the effectiveness and adaptability of data protection frameworks in the face of a rapidly evolving digital economy. By exchanging knowledge and insights, DPAs can share best practices, learn from one another's experiences and stay up to date on emerging challenges, strengthening the enforcement.

5. Conclusion

DPAs are cornerstone institutions in data protection legal frameworks, playing a crucial role in upholding fundamental rights related to the processing of personal data and ensuring adherence to data protection regulations. Particularly in populous nations such as Nigeria and Brazil, managing vast amounts of personal data processing while addressing the diverse needs of their populations adds significant challenges to the responsibilities of DPAs.

Raising awareness about data protection among citizens and organizations presents an additional layer of complexity, as it must account for varying levels of technological access, organizational maturity, education, and understanding across different demographic groups, particularly children, teenagers and the elderly. DPAs have an enormous task in not only monitoring compliance with legislation, but filling gaps that the regulation itself leaves to these authorities. Regulatory construction by DPAs is fundamental considering that data protection laws have gaps that need to be filled, especially regarding the adequacy of practices by controllers and processors.

Due to this context, international cooperation emerges as a very useful tool for DPAs. As personal data increasingly transcend national borders, collaboration among regulatory bodies becomes indispensable, enabling them to exchange knowledge and experiences. In an increasingly digital and interconnected world, collaboration between DPAs is essential to protect the privacy rights of individuals and ensure the responsibility of organizations in relation to the processing of personal data. Institutional partnerships are of great importance for fulfilling the mission of data protection authorities as it allows the exchange of practical knowledge between institutions.

Moreover, considering the provisions outlined in both the NDP Act and the LGPD, fostering a close relationship grounded in mutual cooperation between DPAs is not only feasible but actively en-

couraged. Both the NDPC and the ANPD converge in advocating the promotion of international cooperation between authorities .Such cooperation facilitates the alignment of enforcement actions, fosters consistency in regulatory standards, and ensures that data protection frameworks remain effective in a rapidly evolving, data-driven global economy.

To enhance their effectiveness, the NDPC and ANPD should focus on promoting international cooperation for exchanging best practices, harmonizing standards, and facilitating cross-border data transfers, which can even potentially lead to an adequacy decision between Nigeria and Brazil. Both authorities should also prioritize developing context-specific guidelines to support businesses of varying sizes in achieving compliance while addressing local needs. By working together, DPAs can mutually address their challenges more effectively, which can even result in the issuance of an adequacy decision to enable international data transfer between countries. The advances of the NDPC and ANPD until now demonstrate in practice how both can contribute in this scenario.

Works Cited

Autoridade Nacional de Proteção de Dados. "Autoridade Nacional de Proteção de Dados e Secretaria Nacional do Consumidor Lançam 'Como Proteger Seus Dados Pessoais'." Autoridade Nacional de Proteção de Dados, 2023, https://www.gov.br/anpd/pt-br/assuntos/noticias/autoridade-nacional-de-protecao-de-dados-e-secretaria-nacional-do-consumidor-lancam-201ccomo-proteger-seus-dados-pessoais201d.

Autoridade Nacional de Proteção de Dados. "ANPD Publica Guia de Segurança para Agentes de Tratamento de Pequeno Porte." Autoridade Nacional de Proteção de Dados, 2023, https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-guia-de-seguranca-para-agentes-de-tratamento-de-pequeno-port.

Autoridade Nacional de Proteção de Dados. "Regulamentações da ANPD." Autoridade Nacional de Proteção de Dados, 2023, https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-

normativos/regulamentacoes_anpd.

Autoridade Nacional de Proteção de Dados. "ANPD Assina Memorando de Entendimento com a Agência Espanhola de Proteção de Dados." Autoridade Nacional de Proteção de Dados, 2023, https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-assina-memorando-de-entendimento-com-a-agencia-espanhola-de-protecao-de-dados.

Autoridade Nacional de Proteção de Dados. "ANPD e o Comissariado Canadense para a Proteção da Privacidade Firmam Memorando de Entendimento." Autoridade Nacional de Proteção de Dados, 2023, https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-o-comissariado-canadense-para-a-protecao-da-privacidade-firmam-memorando-de-entendimento.

Center for Information Policy Leadership. "Eight Privacy Priorities for 2020 and Beyond." Center for Information Policy Leadership, 2020, https://www.informationpolicycentre.com/cipl-blog/eight-privacy-priorities-for-2020-and-beyond.

Doneda, Danilo. “Da Privacidade à Proteção de Dados Pessoais: Elementos Da Formação Da Lei Geral de Proteção de Dados”. 2nd ed., Thomson Reuters Brasil, 2019, pp. 185-186.

European Data Protection Board. "EDPB Adopts Statement on DPAs' Role in the AI Act Framework & EU-US Data Privacy Framework FAQ." European Data Protection Board, 2024, https://www.edpb.europa.eu/news/news/2024/edpb-adopts-statement-dpas-role-ai-act-framework-eu-us-data-privacy-framework-faq_en.

Global Privacy Assembly. "Strategic Direction, Mission, and Vision." Global Privacy Assembly, 2023, https://globalprivacyassembly.org/the-assembly-and-executive-committee/strategic-direction-mission-and-vision/.

Greenleaf, Graham, and Bertil Cottier. "International and Regional Commitments in African Data Privacy Laws: A Comparative Analysis." Computer Law & Security Review, vol. 44, 2022, p. 105638, doi:10.1016/j.clsr.2021.105638.

Nigeria Data Protection Commission. “Nigeria Data Protection Annual Report 2023”.

OECD. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. OECD Publishing, 2002, https://doi.org/10.1787/9789264196391-en.