

Roles and Effectiveness of Information Policy Regulatory Bodies and the Safeguard of Public Interest in Nigeria.

**Muhammad Bala KASIM¹, Sophia Vivian ADEYEYE²,
Yahaya Abdullahi ISAH³, & Amina IBRAHIM⁴**

^{1,3}University Library Services, Federal University of Technology, Minna, Nigeria.

²Department of Information Management, Lead City University, Ibadan, Nigeria.

⁴Niger State Library Board, Minna, Nigeria.

+2348089892369,mbnas83@gmail.com¹; +2348061127708,sophia.adeyeye@lcu.edu.ng²;

+2347037152106,yahaya.isah@futminna.edu.ng³;

+2348060200153,ibramina83@gmail.com⁴

Abstract

Information policy is a set of rules and regulations guiding the creation, storage, access, use and dissemination of information. This paper discusses the concept and importance of information policy/information security policy. It also identified the relevant stakeholders as well as regulatory bodies in the information policy implementation process such as ministries departments and agencies of government in Nigeria. The paper adopted a theoretical approach by adopting and explaining the public interest theory or regulation in the context of information policy objectives. Exabeam pie chart as well as Rowe's corroborative view on objectives of information policy was highlighted. Roles of information policy regulatory bodies were discussed. Some related studies on effectiveness of information policy implementation were clearly stated. Several hindrances to effective implementation of information policy in Nigeria were identified. The study concluded that Information policy or Information Security policy is aimed at ensuring equitable access to information by the public while ensuring safety and protection of information or data classified as harmful or potentially harmful for public consumption. To ensure the true effectiveness of the policy, the stakeholders involved in the implementation process must clearly state the policy direction or purpose it seeks to achieve, adequate and updated technological infrastructures, avoid compromise as well as inter-agency rivalry among the implementation agencies in Nigeria.

Keywords: Information Policy, Information Security, Regulatory Bodies, Public Interest

Introduction

Information policy is a set of rules and regulations guiding the creation, processing, storage, access and dissemination of information. Information policy and information security policy are often used interchangeably by different authors to mean the same. Information security policy according to Anwita (2024) is a set of rules, practices, guidelines, and processes that governs the management, protection, and access of information. It ensures the confidentiality, integrity, and availability of networks, applications, systems, programs, and data across the infrastructure. Yahaya et al (2019) defines Information policy as any written or unwritten law, regulation, rule or practice that affects the creation, acquisition, organization, dissemination

or evaluation of information. Information policy seeks to address the concerns of unguarded creation, access and dissemination of information to the public. Information policy according to braman (2011) is a policy that is comprised of laws, regulations, and doctrinal positions – and other decision making and practices with society-wide constitutive effects – involving information creation, processing, flows, access, and use.

Information policy is a set of interrelated principles, laws, guidelines, rules, regulations, and procedures guiding the oversight and management of the information life-cycle: the production, collection, distribution/dissemination, retrieval, and retirement of information. Information policy also embraces access to, and use of, information. Collectively, policies form a framework that profoundly affect[s] the manner in which an individual in a society indeed a society itself, makes political, economic, and social choices (Hernon & Relyea, 2003). One of the cardinal principles of information policy is not to deny users access to information or data but, it ensures that information or data that are meant for general public are made accessible regardless of educational, social and economic status of information consumers, while ensuring that information/data that are classified as private or confidential are only made accessible to authorized users. In a simple tense, information policy ensures equitable access to information.

The importance of information in our society is boundless and so the need to have an implementable guidelines or policies to checkmate the flow of information cannot be overestimated. This is what information policy seeks to achieve. Several stakeholders are involved in the information policy making process. These stakeholders are spread across government and private sectors to ensure direct restriction, encourage or otherwise regulate the flow of information across the nooks and crannies of our societies. These stakeholders include government ministries which according to Yusuf (2007) include Federal Ministry of Information, Youth and Culture; Federal Ministry of Education; Federal Ministry of Science and Technology; Federal Ministry of Tourism; Federal Ministry of Transport and Aviation; Federal Ministry of National Planning; Independent Electoral Commission and others. The departments and agencies handling issues of both government and private (individual) data and information includes Federal Information Centre, National Orientation Agency, National Library of Nigeria, National Bureau of Statistics, National Population Commission, Nigeria Communication Commission, Nigeria Data Protection Commission, National Information Technology Development Agency, Public Institutions and Registries charged as custodians of government and personal data of citizens in Nigeria.

Regulatory bodies or agencies are independent governmental body established by legislative act in order to set standards in a specific field of activity, or operations, in the private sector of the economy and then to enforce those standards. Regulatory agencies function outside direct executive supervision. Because the regulations that they adopt have the force of law, part of these agencies' function is essentially legislative; but because they may also conduct hearings and pass judgments concerning adherence to their regulations, they also exercise a judicial function, often carried out before a quasi-judicial official called an administrative law judge, who is not part of the court system. Regulatory agencies became popular means of promoting fair trade and consumer protection as problems of commerce and trade became more complex, particularly in the 20th century (Britannica).

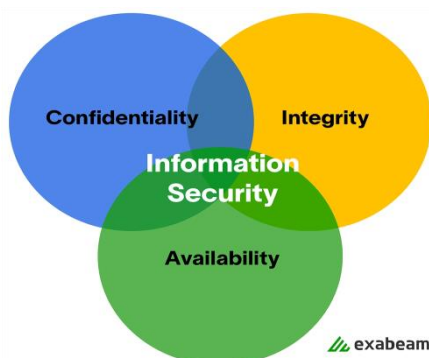
Review of Literature

Theoretical Framework- The Public Interest Theory of Regulation

The public interest theory of regulation claims that government regulation acts to protect and benefit the public. The public interest is "the welfare or well-being of the general public" and society. Regulation in this context means the employment of legal instruments (laws and rules) for the implementation of policy objectives. Public interest theory competes for acceptance with public choice and regulatory capture in explaining regulation and its effects on public welfare (Hantke-Domas, 2003).

The Nexus between Public Interest Theory of Regulation and the Information Policy Objective

This theory propounds that "government regulation acts to protect and benefit the public". In the context of information policy and public interest therefore, the theory seeks to ensure that legal instruments (laws and rules) put in place by the government will be of benefit and protection for the public as owners and users of (personal and other) information. What it means is that the policy put in place ensures equitable access to information by the public while assuring that the policy also provides full support for privacy and protection of their personal data/ information. Thus, the public interest theory of regulation establishes acts for safeguarding welfare or well-being of the public with respect to fair and impartial access to information and protection of their personal data/information.



Adopted from Exabeam(n.d) on <https://www.exabeam.com/explainers/information-security/the-12-elements-of-an-information-security-policy/>

While emphasizing on the elements of information security, Exabeam identified that information security focuses on three main objectives as shown above:

- **Confidentiality:** Only authenticated and authorized individuals can access data and information assets.
- **Integrity:** Data should be intact, accurate and complete, and IT systems must be kept operational.
- **Availability:** Users should be able to access information or systems when needed.

These above objectives were also corroborated by Rowe (2017) that the objective of an information security policy and corresponding program is to:

1. Protect the organization, its employees, its customers, and also vendors and partners from harm resulting from intentional or accidental damage, misuse, or disclosure of information;
2. Protect the integrity of the information; and
3. Ensure the availability of information systems.

The Roles of Information Policy Regulatory Bodies

A good information policy is expected to be featured by the following roles:

1. Provision of nationwide or global access to relevant information/data through various public institutions especially information about government programmes, procedures and policies. This is provided for in the Freedom of Information (FOI) act.
2. Educate the citizens on how to organize, store and manage personal data and information
3. Ensures that individuals and organizations that possess sensitive information/data protect it from unauthorized access.
4. Through the Nigeria Data Protection and Regulation (NDPR) individuals and organizations (Financial institutions) are made to comply with laws surrounding the private data protection to prevent cybercrimes and related threats.
5. Protect the intellectual property rights of authors, researchers, academics and artisans. This is achieved through Nigerian Copyright Act (NICA).
6. Increases international collaboration and co-operations among different countries. This is enhanced through cross-border data flow between the co-operating countries.
7. Provides guidance for libraries on how their users make ethical use of information resources in the libraries.
8. Enacts penalties and other legal actions against violators of information policy.

Studies on Effectiveness of Information Policy implementation by Regulatory Bodies

Implementation of information policy means execution of laws or regulations contained in the information policy document. It ensures that the objectives of the policy are fully attained. Effective implementation of information policy varies from one country to another. In some countries, implementing information policy is highly effective due to the system of government and high levels of deployment of information and communication technologies (ICTs) and an active and uncompromised implementation task force. While in other countries, implementing information policy effectively is a mirage. This can be attributed to certain challenges which may include unclear policy direction, compromised policy implementers, political opposition, corruption, lack of continuity and so on.

Certain studies were conducted by different researchers on the effective implementation of information policy in Nigeria. In a study carried out by Anyira (2021) on library and information policy in Delta State of Nigeria, when respondents were asked to give their general rating of the level of implementation of information policies in their libraries. The ratings show very high 11%, high 244%, undecided 25%, low 30%, and very low 10%.

On personal data protection, The Web Foundation and Paradigm Initiative (2017) commissioned a review of the data collection practices in Nigeria, as well as the policies and

regulations in place to govern the collection, protection and use of this data. The findings show that there are five primary concerns around the collection and use of personal data , both online and offline , in Nigeria:

- a. The use of personal data may be incompatible with the purpose for which it was collected;
- b. Individuals have no rights in relation to the collection, use, and storage of their personal information;
- c. Nigerians are not offered adequate opportunities to consent to or opt out of data collection;
- d. There is limited-to-no transparency around the processing of personal data, and there is limited information available around how this personal data is used and stored, leading to greater risk of a personal data breach;
- e. Children are exposed to privacy risks online and often lack the legal capacity to give valid consent, and may unknowingly disclose personal information to online platforms due to the appealing nature of their visual content.

Challenges of Information Policy Implementation

Just like execution of other public policies, implementing information policy to safeguard public interest often faces numerous challenges. The major hindrances are:

Ambiguous/Unclear Definitions and Directions of Policy: Lack of clear definitions and direction in policy definitions and objectives or unclear statement of roles and responsibilities can lead to inconsistent implementation and enforcement. Clear guidelines are essential for coherent policy execution.

Evolving Technologies (Barriers): Rapid technological advancements can outpace policy development and enforcement. This creates gaps in coverage and effectiveness, particularly concerning emerging technologies.

Data Privacy and Security Concerns: Balancing the need for information access with privacy and security concerns is a significant challenge. Ensuring data protection while providing transparency and public access can be difficult.

Insufficient Funding and Skilled Personnel: Effective policy implementation requires adequate funding, human resources, and infrastructure. Budget constraints and lack of skilled personnel can hinder efforts.

Regulatory and Legal Challenges: Variability in laws and regulations across different jurisdictions can complicate policy implementation. Harmonizing regulations while respecting local legal frameworks is a complex task.

Political opposition and Bureaucratic Inertia: Political opposition and bureaucratic inertia can slow down or block policy implementation. Policy changes may face resistance from stakeholders with conflicting interests.

Public Awareness and Stakeholders Engagement: Lack of public awareness and engagement can undermine policy effectiveness. Ensuring that the public understands and supports information policies is crucial for their success.

Interagency Coordination: Effective implementation often requires coordination among multiple government agencies. Interagency rivalries, communication gaps, and lack of collaboration can impede progress.

Economic and Commercial Pressures: Commercial interests, particularly from powerful corporations, can influence policy direction and enforcement. Balancing public interest with economic considerations is a persistent challenge.

Inconsistencies in Information Policies in the Global Arena: Globalization necessitates international cooperation on information policies. Differences in national policies and priorities can hinder coordinated efforts on a global scale.

Complexity and Rapid Change: The complex and rapidly changing nature of information environments makes it difficult to create flexible yet robust policies that can adapt to new challenges.

Absence of Feedback and Evaluation Mechanisms: Without proper metrics and evaluation mechanisms, it is hard to assess the effectiveness of information policies. Continuous monitoring and assessment are necessary for iterative improvements.

To corroborate the above, Aminu, et al. (2021) enumerate certain challenges to information policy implementation to include:

1. Lack of clear definition of responsibility and coordination
2. Lack of participation of stakeholders in the implementation process
3. Lack of involvement of professionals in the implementation process
4. Lack of continuity commitment to policy
5. Disagreement between the implementers, conflict during implementation and compromise
6. Over-ambition/ambitious in policy formulation
7. Corruption
8. Lack of foresight

Conclusion

Information policy or Information Security policy is aimed at ensuring equitable access to information by the public while ensuring safety and protection of information or data classified as harmful or potentially harmful for public consumption.

Recommendations

The following recommendations are proffered for a functional and inclusive implementation of information policy by the regulatory agencies in Nigeria

1. To ensure the true effectiveness of the policy, the stakeholders involved in the implementation process must clearly state the policy direction or purpose the policy seeks to achieve.

2. Adequate and updated technologies as foresight mechanisms for handling ever-emerging access to information
3. There should be a strong synergy and avoidance of inter-agency rivalry among the implementation agencies in Nigeria.
4. Avoidance of compromise and nepotism when it comes sanctioning defaulter of information policy by the implementation agencies.

REFERENCES

- Aminu, M. U., Aliyu, D. A., Sekinat, J. & Abubakar, M. M. (2021). Information policy implementation in Nigeria: Issues and Challenges. A Paper Presented at the Seminar Series Session of Ahmadu Bello University Library Complex Held on 10th August at PG E-Library, Kashim Ibrahim Library. Pp 7-10.
- Anwita, (2024). Understanding Information Security Policies: Importance & Key Elements. <https://sprinto.com/blog/key-elements-of-information-security-policy/>
- Anyira, I.E. (2021) Implementation of library and information policies in libraries in delta state, Nigeria. Unpublished article.
- Braman,S.(2011). Defining information policy. *Journal of Information Policy*. 1:1-5.
- Britannica, The Editors of Encyclopaedia. "Regulatory agency". Encyclopedia Britannica, Invalid Date, <https://www.britannica.com/topic/regulatory-agency>. Accessed 13 May 2024
- Hantke-Domas, M. (2003). The Public Interest Theory of Regulation: Non-Existence or Misinterpretation?". *European Journal of Law and Economics*. **15** (2): 165–194.
- Hernon, P. & Relyea, H.C. (2003). Information Policy. In *Encyclopedia of library and information science*. New York: Marcel Dekker, Inc.
- Rowe, B.(2017). Characteristics of a successful information security policy. Retrieved from: <https://www.linkedin.com/pulse/characteristics-successful-information-security-policy-branden-rowe>
- The Web foundation and Paradigm Initiative (2017). Personal data protection in Nigeria, the webfoundation retrieved from: [http:// bit.ly/nigeriadataprotection](http://bit.ly/nigeriadataprotection)
- Yahaya, D., Ejigbo, DS., Oladokun, BD (2019). An overview of national policy on information in Nigeria. *International Journal of Academic Librarianship and Information Science* 7(6): 166-173
- Yusufu, A (2007). An overview of Nigeria information policy. *Samaru Journal of Information Studies Vol. 7 (1)*. <https://www.exabeam.com/explainers/information-security/the-12-elements-of-an-information-security-policy/>