MANAGING IDENTITY DIVIDE: LANDSCAPING THE CONSTRAINTS OF THE NIGERIAN IDENTIFICATION SCHEME

Olubunmi David APELOKO
Department of Public of Administration, Obafemi Awolowo University,
Ile-Ife, Nigeria

Gbeminiyi Kazeem OGUNBELA
Department of Public Administration, Federal Polytechnic Ilaro, Nigeria;
Ilaro, Nigeria
gbeminiyi.ogunbela@federalpolyilaro.edu.ng

Toyin Labake OGUNBIYI
Department of Public of Administration, Obafemi Awolowo University,
Ile-Ife, Nigeria

Abstract: *The spontaneous advancement in information communication technology aided several achievements in the way and manner government transacts business with citizens and private businesses. As such, the adoption of e-government in both public sector and private sector is attached to the growing wave of identity management across the globe. As it is practice in the public sector, policy intervention was adopted to manage the deployment of national identification schemes and this is applicable to Nigeria. However, a decade and half implementation of the policy yielded no significant results given the huddles of enrollment faced by an average enrollee. It was on these grounds that this article to investigate the constraints navigating the operation of the national policy and framework on identification system in Nigeria becomes researchable gap. Survey research (questionnaire and interview) and descriptive statistics (Relative Impact Index) were used in collecting and analysing data gathered from 214 administrators of four relevant identity-oriented agencies (NIMC, NIS, INEC and FRSC). The results indicated that constraints such as insufficient central database infrastructure, unstable electricity, poor internet connectivity, unclear delegation of responsibilities among agencies, insufficient funding and institutional corrupt practices were principal among the constraints of the new identity regime. It further concluded that more research of this nature is expected to explore the emerging issues from the implementation of the policy while advising the government to rework the identified constraints, for instance, it is expected that government decentralise the enrollment process following the model used in the telecommunication industry for registering SIM cards by accrediting private firms for the enrollment exercise. It added that for the system to be unique and foundational as claimed in the policy thrust, the policy guidelines on harmonisation and integration of existing functional database need an accelerated redevelopment for implementation as well as a separate legal instrument footing its legality.*
Keywords: *Policy, biometric, Identity, identification system, identity management, implementation*

INTRODUCTION

The spontaneous advancement in information communication technology aided several achievements in the way and manner government transacts business with citizens and private businesses. Identification system allows the arrangement to be made for more government ministries to provide e-services to the public (Arora, 2008: Naumann, 2008).

More specifically, UN Development Index Survey released in 2016 noted that more countries use e-identification as part of criteria to access online or mobile services. This new development was however linked to the government agencies in order to provide citizens-focused e-services. Originally, the adoption of electronic identification in the provision of e-services is sharply linked to the principle of new public service movement. This principle states that the provision of public services should be based on egalitarian and equal right ideology (Denhardt & Denhardt, 2007). This means that for services to be provided equally, numbers and identities of citizens are vital to the government especially for planning purpose. Again, the term such as "digital governance", "the paradigm of population data" added more weight to the significance of identification scheme (Dunley, Margetts, Baslow & Tinkler, 2006; Rahardjo, 2016). The importance of identification system in public service is more strengthened by the argument of Khatchateuror and Laurent (2014) that adoption of e-government in public sector and private sector is attached to the growing wave of identity management across the globe. Castro (2011) remarked that e-services are rendered by government and private businesses via identification system. For instance, Millard and Carpenter (2014), Castro (2011), Vassil et al (2016) and Kalvet (2012) cited that services such as "tax-on-web" in Belgium, "e-voting" in Estonia, "my people services" in Denmark, were deployed through the instrumentality of identification system. Studies have shown that e-identification has been extensively deployed in European centuries. This necessitated the introduction of an European Citizen Card (Castro, 2011). UN Survey (2016) posited that in order to identify and render governmental services to citizens and the business sector and reduce the cost of governance, thus, the implementation of identity management system is inevitable.

In the case of national policy on identity management system in Nigeria, available evidence has shown a low level of implementation. Comparatively, India started the enrollment process of her citizens in 2009, and has since captured 940 million Indians out of 1.2 billion people representing 78% (Asian Development Bank, 2016). Meanwhile, in Indonesia, 140 out of 252 million Indonesians representing 56% were captured within two years; 100 million in 2011, 40 million in 2012 (Asian Development Bank, 2016). Invariably, one could see that after 10 years of commencement in Nigeria, the system is struggling to capture less than a quarter of the Nigeria population. According to World Bank (2018), Nigeria population growth rate is put at 2.6%, therefore, the population is expected to grow at a minimum of 5 million persons per annum, thereby widening the gap between the enrolled and un-enrolled Nigerians. In addition, another issue affecting the implementation of the policy might be the delay experience in the production of the GMPCs. The production of these cards occupied a fundamental spot in the process of deploying the national identity management system. However, the World Bank reported that in 2015, only 418,000 GMPCs were issued as against 12 million GMPCs proposed in the first year of implementation. This figure is 6.8% of 6.1millions NINs already assigned as at 2015. These discreditable figures could be traced to the staggered manner in which the GMPCs are being produced and distributed. This policy output deviated from the policy target of distributing at least 12 million GMPCs to Nigerians in the first year of implementation. All these evidence indicated that there are clogs hindering the implementation of the policy as proposed in Nigeria especially in the area of citizens' enrollment and harmonisation of functional databases. This poses a threat to the policy objective of ensuring interoperability among government institutions as the numbers of

identities captured and databases integrated do not guarantee provision of all-inclusive e-government services. It was on these grounds that the need to investigate the constraints navigating the operation of the national policy and framework on identification system in Nigeria becomes researchable gap.

LITERATURE REVIEW

The term identity has been diversely conceptualised along different perspectives by several authors. Etymologically, the word identity is derived from a Latin word 'Idem' meaning "sameness, oneness, and state of being the same" (Wiktionary, n.d). This naturally means that identity is the ability to remain the same or identical irrespective of the location of the persons or objects involved, which means no individual can assume different identities at the same time. In this study, the identity of an individual as a member of a society is a major concern. Therefore, in order to aptly operationalise the concept of identity as used in this study, views of scholars on what constitutes identity were visited, though varied. The nebulosity in the definition of identity was established by Sullivan (2011) where it was stressed that the definition of identity has always been without exactitude; that is identity equals identity depending on the context and nature of the phenomenon in which such definition is given. This means the term identity could possibly be used differently in several fields of study. Identity according to Sullivan (2011) is a set of adopted information that is legally and statutorily driven under the enforcement of a government implementation mechanism. According to Mostov (1994), identity of an individual is a mirror image of his characteristics naturally noticeable by members of the community in which he resides while Ayamba and Ekanem (2016) defined identity from an information management angle as an embodiment of biophysical attributes which aid an individual to access bespoke benefits in an internet aided environment or in public places. By implication, however, it means that the identity of individuals in any society could be linked to the accessibility of public services electronically. Similarly, identity is defined based on components it entails – socio-demographic attributes; benefit oriented behaviour driven by shared value in multicultural settings; pattern of lifestyle activities such as travel pattern, consumption of public services; historical component of individual relationship with the public (state and individual) especially in purchasing decisions, tax obligations and participation in socio-political activities (Future of Identity in the Information Society Project, 2006)

In a clearer view, series of definitions of identity have been succinctly captured in a joint report issued in 2003 by the Independent Centre for Privacy Protection (ICPP) of Germany and Studio Notorile Genghini (SNG) of Italy. Identity to them can be defined from three perspectives namely sociological, legal and technical. Sociologically, identity is defined in reference to differences in public and private appearance of a person. It is the combination of the realisation of personal liberty and social attributes of the person. Identity equals the interface of a pre-lingual instance of the individual that supports social integration. The decision about a point in time for initiation of a personal trait or the blend of attributes in past, present and the corresponding summary of attributes that are uniquely captured is viewed as identity (ICPP and SNG, 2003). Technically, identity is conceptualised from an electronic point of view to mean all personal oriented data that can be kept and routinely interlaced by computer-based solutions. It represents much more

genuine ascription of properties to an individual that is designed to enable real-time accessibility for instantaneous operation (ICPP & SNG, 2003). The legal definition of identity derived it source from codifications of rights and obligations in the constitution or law of the society. For instance, ICPP and SNG (2003) operationalised the legal aspect of identity to connote establishment of person's obligations, rights, and privileges apportioned by existing legal system and constitution of a state. It answers questions on matters affecting identification and verification of individual rights and obligations. Analysis from the above definitions shows that identity is encapsulated in three-folded layers which involve social attributes, legal privileges and electronic accessibility of public services embellished in a single platform. For instance, World Bank Country Assessment Report (2015) stressed that the arrival of innovative technologies such as the internet, social media, digital solutions, and mobile telephone necessitated the designation of a digital method of identity, that it is a cross-sectorial solution providing a sole identity for accessing public service across multiple sectors.

Identity viewed from electronic parlance means a digital edify that provides means of affirming who people claim they are, as a result, give them accessibility to an array of public goods and services. Electronically, identity in the public realm allows one person to access services provided across numerous sectors such as social security, tax administration, education, banking, and financial services as well as performs other personal roles. Thus, legal coverage is required to regulate the protection and control over identity data in an independent manner (European Union Discussion Paper, 2006). Another comprehensive definition of identity was given in Greenwood (2007) cited in Lips and Pang (2008:12) as a three-legged topology was set while defining identity; the digital identity (such as username, IP, email address); the physical identity (such as passport, driver's license); the converged identity, a combination of the digital and the physical identity. In OECD (2007), identity from a physical realm is considered to involve perhaps a broad set of individual physiognomies by which a person is captured while in the electronic world; an identity can be simply regarded as a subclass of an individual's identity data. This study, therefore, defines identity as the ability of a person to prove the genuine existence of his or her biophysical attributes manually or electronically. It is a legally and generally accepted electronic distinguishable characteristic of a person or an entity defined in an identity management system of a country. It consists of biometric and fingerprint data of individual or legal features of an organisation that is in electronic or digital form. Henceforth, identity, as used in this article, means biometric and physical attributes of an individual codified into a verifiable platform electronically or manually.

Identification is a vital element in the interfaces existing among citizens, governments and private institutions in an organised state. An efficient means of establishing one's identity guarantees ability to exercise and access certain rights, privileges and access range of public services; as such an ineffective identification mechanism could jeopardize the principle of efficiency and effectiveness that are required of any responsible and responsive government (World Bank Digital Identity Toolkit, 2014). According to Jaide (2010) identification is the process that confirms social and physical attributes of an individual as a citizen of a country or society that qualifies such person to access certain government services through a distinctive identification token. More so, identification is the course of recognizing and establishing similarity and dissimilarity of the identity of a particular person or entity (Concise Oxford Dictionary)

while Clarke (1994) sees identification as the act of making a semblance of a thing or an entity same or identical. Therefore, identification of human being is the connection between the characteristics of the human and the being himself. In modern government and administration, therefore, the concept of identification is a daily terminology that is used by officials of public and private institutions in discharging their duties to the public. They ensure that any individual or legal entity accessing or providing public services such as banking and financial services, legal services, export and import businesses, the award of government contracts and other public-oriented services proves the authenticity of his identity. Identification in identity management is not only for natural persons but also artificial persons – corporate entity recognised by law as a separate individual (Ojaide, 2010). Identification and identity management, though a thin demarcation exists between the two terms, the latter is more encompassing, perhaps in definition and practicability. According to Ayamba and Ekanem (2016), identity management as a concept frequently appeared in the practice and literature, yet a victim of conceptual infancy. That is, no definition is accepted as a widely acclaimed conception that really captures what identity management is. For instance, Scorer (2007) described identity management as the combination of sets of business-oriented procedures and auxiliary infrastructure for the formation, preservation, and deployment of digital identities, while Crompton (2004) attested identity management to mean a set of information management structures and practices designed to promote assurance in verifying identities of individuals. From these definitions, identity management could be described as the application of new public management in managing individual's data and identity.

According to ICPP and SNG (2003), identity management from a sociological perspective is better named as identities management; it deals with administering and supervising possible forms of participation in a standard manner in order to differentiate social situations and methods of addressing them. This definition expanded identity from one-off meaning to involve all possible attributes that might be demanded by diverse situations. Legally, identity management is not well received. It is limited to the technological environment; not regulated by legislation as an organic entity; it involves establishment of subjects' reference points for rights and obligations while technically, identity is seen as numbers, directly or indirectly notating an object, a person, a device or a corporate entity (ICPP and SNG, 2003). For Lips and Pang (2008), identity management seems to attract technical definitions; that is, ample existing conceptions captured identity management from technological sensational perspective. According to Burton Group (2003) reported in Scorer (2007:43), identity management combines business procedure, and enabling infrastructure configured to ensure maintenance and usage of electronic identities while Brands (2002a) defined identity management as "management of identity-related information … simply the digital authentication and certification of identity - related information, with its biggest use in access management". These definitions share a similar stand, that is, identity management cannot be conceptualised without permitting a semblance of data management, and digital technologies to appear in the context and in the text. On the contrary, Lips and Pang (2008) negated their earlier view. They argued that the definitions were too digitized, stressing the fact that digital appearance of citizens, though real, still exists in abstraction. People still relate with government agencies as social-being through one form of digital identity or the other. Hence, the social context in which people relate with the government agencies cannot be wished away. For instance,

results from past studies in European countries indicated that public trust combined with socio-cultural tendencies cum historicity of citizens, to a meaningful extent predict acceptance and usage or otherwise, of any identity management applications (Prime, 2004; Mckenzie, 2008).

Essentially, it appears that placing a definition on identity management is more tasking than it seems to be, combining blocs such as physical and digital viewpoints; administrative principles like impartiality, equity, e.t.c; and socio-cultural attributes cum historicity of a state might provide a near-generally accepted definition. This study, however, views identity management as the application of administrative principles to electronically define socio-cultural and historical uniqueness of individuals and entities for the purpose of authenticating and verifying identities in the conduct of day to day activities. Authors have shown concern about fragmented conceptions of identity management system as the need to standardise and internationalise what constitutes identity management system is endlessly growing (Greenwood, 2007; Durand, 2003). It has been argued that given the diversity in economic, political and organisational peculiarities of different spheres, placing a generally accepted description of identity management system on institutional basis appears to be an unattainable fit (Backhouse 2006; Backhouse, Hsu & McDonnell, 2003). For instance, NIMC (2011) described identity management system as the combination of biometrics and demographical characteristics in a systematic approach with a view to authenticating and diversifying individual unique identifier. According to Claub (2001), identity management system is a set of interconnected technologies that empower operators or users to manipulate types and quantity of personal information released, while Ibrahim and Abubakar (2016) gave a related view of identity management system – it is information management system-like architecture with capacity to provide a networked identity management.

In a similar way, identity management system is seen as privacy technological innovations that allow the individual to protect his identity in an environment that is controlled by an external party with a view to anonymously authenticating his identity (David, 1985). A deep reflection of the views raised above gave an impression that the identity management system is defined based on what it does. However, these definitions appear too casual, as efforts were not made to reflect elements of the system since what is being conceptualised is a system. From here, Lip and Pang (2008) reported that Higgin, an internet-based company defined identity management system as a system that:

- Provides a manner in the management of personal identity data.
- Allows users to have control over their personal data circulated among government information terminals
- Provides an information model for electronic identity-related information as well as security safeguard for numerical access points or terminals
- Creates an electronic connector for providing access to registries communication channel, interoperability and databases among established institutions within an integrated framework
- Retains element of social interaction among users of identity-driven applications

More importantly, Cameron (2006), an architect with Microsoft offered what is conventionally termed “7 laws of identity” to describe Identity management system with the following element:

- User control and consent: the system must not disclose users' identity-related data without the users' consent.
- Minimal disclosure for a constrained use: in the event of disclosure, the system is expected to demonstrate refrain in releasing sensitive identity-related information.
- Justifiable parties: this must be able to identify genuine parties legally designed to have access to identity information.
- Directed identity: a good identity system should provide enablers for both multi-directional locators for public institutions and one-off identities for individual firms with the primary aims of managing issues relating to storage and historical transactions.
- Pluralism of operators and technologies: an efficient identity management system should be multi-centric by allowing inter-networking of several identity solutions operated by identity-driven entities.
- Human integration: the system must be aware of human nature of the users embedded with an interface that combines peculiarities of human and electronic device for smooth interaction. This, of course, will deepen predictability of the entire system.
- Consistent experience access context: the system created must be consistent and stand the test of time to become part of the world order without prejudice in the roles its offers the society.

The description above appears analytical, still alluded to the earlier position maintained that identity management system has mostly to be defined on the basis of what it consists. Again, Clark (2004) identified the following as the attributes of an identification system:

- The universality of coverage: it must be able to capture all eligible users.
- Uniqueness: two persons must not have the same identity.
- Indispensability: the system must be available all the time.
- Collectability: the system should be able to issue individual identifier without any form of delay.
- Storability: the system must be able to store a transactional history of users.
- Permanence: the system must not allow each identifier issued to be manipulated or changed.
- Exclusivity: the system should host the database hub for every identifier in the system as such no need for the creation of a parallel identification system.
- Precision: the system should process the transaction with accuracy and absence of mistakes.
- Simplicity: transmitting and recording identifiers should be simple and easy.
- Cost: the system should be cost-effectively designed.
- Convenience: the system should operate in a less time-consuming manner.
- Acceptability: the system should be socially and generally in consonance with social norms.

These features attempted to perfectly capture the identification system by featuring a system that is all encompassing. Furthermore, Duncastle (2015) explained identity system as "the set of laws, standard supervision, and facilities that can contain one or more-ID means (and their systems) and are acknowledged as a national facility by the corresponding country". Hansen, Krasemann, Krause, & Rost (2003) equally attempted to converge on

what identity management contains by proffering the following requirements of identification systems:

- : this connotes the ability of IMS to administer, manage and maintain identity resources in an efficient and productive manner. This includes the establishment of reliable and effective communication channels among parties in the system.
- Usability: this is another prerequisite for an efficient IMS, it requires the system to be usable to every normal user.
- Security: this criterion requires that an IMS is built in such a way that it will safeguard the integrity, availability, and confidentiality of the system.
- Privacy: this is important in order to comply with the existing privacy laws & rules guiding management of identity-related information as such the system should accommodate privacy-enhancing technologies (PET).
- Law Enforcement: this system is expected to strike a balance between protecting the privacy of personal entity-related data and providing state law enforcement agencies access to personal data of the public.
- Trustworthiness: this criterion believes that for an identification system to be generally acceptable, members of the public must be able to accord unreserved trust in the system where the personal data will be kept.
- Affordability: the cost of gaining access to IMS resources by the public should not be high. The system should be made available to the public considering the long-term benefits.
- Interoperability: this is a major prerequisite if not the most important. It drives the IMS environment by harmonizing existing identification schemes into one system that is accessible by the functional systems.

Developing an identity management system is a herculean task that requires careful planning and implementation. Gelb and Clark (2013) remarked that creating an identification system that has large-scale applications usually come with dire challenges, which make the process complicated. In a general assessment of the challenges affecting the implementation of identification system of 43 countries drafted from all continents, Anderson *et al*. (2016) identified certain challenges. The study reported corruption of varying degrees affects the implementation of identity management programmemes in many countries. This is said to occur at the micro and macro levels. This is subdivided into: (i) Local extortion of citizens by official and enrollment officers (ii) Collusion between public officials and (iii) Inappropriate procurement of equipment. The study revealed that concerns about the privacy of information hinder rapid implementation of the identification system. It is believed that there is the possibility of abuse of personal information of the citizens. The report shows that the issue of data maintenance is affecting the implementation of an identity management system. Also, the absence of central database infrastructure and inadequate data protection measures affect installing of identification system. Another factor that hinders drive for holistic and comprehensive implementation of the policy is enrollment politics. Here, inadequate access to resources like insufficient equipment and material, limited human resources, lack of logistical support, lack of public awareness were cited. Also complex enrollment procedures like printing and physical mailing of applications and ID card as well as a lengthy feedback process were identified. Risk of critical mass exclusion was also established among the challenges of implementing identification system. The study identified poor coverage as a limiting factor. Issues such

as insufficient enrollment and distribution centres, cost of enrollment (hurdles, long guess, long distance), exclusion of vulnerable groups (poor, rural dwellers, women: refugees) from enrollment suggests that the policies on biometric identification might have come into force without corresponding politics in these countries. Similarly, the financial implication of funding identity management programme also constitutes a challenge to implementation of identification system as claimed in this previous work. This includes insufficient funding by the government and dwindling financial support from international partners and high cost of training and building technical capacity. Staggered harmonisation of esixting identity programmes was also identified among the countries studied. This factor affects the full implementation of an identity management system, as there is always challenges of integration and interoperability of databases. Here, issues like lack of clear delegation of responsibilities and legal frameworks were also identified.

THEORETICAL FRAMEWORK

This article reviewed the Actor-Network Theory and Institutional Theory. These theories were reviewed due to their explanatory strength on the adoption of modern technologies in administrative spheres with specific explanation on the implementation of new technologies. The Actor-Network Theory (ANT) is often time associated with many scholars. The findings and works of the scholars have continued to give relevance to the theory. The works and efforts of Callon (1999); Callon and law (1997); Hassard, Law, and Lee (1999); Latour (2005); Law (1992); Brown (1994); Neyland (2006) gave a strong intellectual backing to the Actor-Network Theory (ANT). Actor-Network Theory (ANT) is a theoretical approach, which describes and explains the complexity in our socio-technical world. It is largely, a holistic approach in explaining activities within our socio-technological world. This theory view activities within the society or the environment with a broader lens, as it sees the actors within a network by looking both human and non-human actors. Administratively, the theory can be said to the summation of the integral view of administration and the system theory. The integral view of administration sees the administration as the activities of "everyone" in the organisation, while the Bertalanffy's system theory also takes cognisance of the various sub-systems (actors) in a network or system. ANT also looks at the collective activities within a system, recognising the activities of subsystem including animate and inanimate elements required to achieve the required goal. For instance, in the work of Latour (1996:373), Callon and Latour (1981:286), the scholars gave a wider definition of an actor as "anything provided it is granted to be the source of action". Every network will only be effective through the actions of all actors – both human and non-human elements.

ANT emphasised relationship, cordiality, and connection between human and non-human in a real-life situation. One cannot work without the other, that is human actors cannot work without non-human actors and the non-human actors will not function without the human actors. According to the theory, actors must be made, re-made, used and re-used to avoid systemic failures. The above point explains the formulation of a policy (making of actors); implementation of policy (using of actors); evaluation of policy (re-making of actors); continued implementation of the policy (re-using of actors). However, the theory does not respect the power of human rather sees it as part of the system that cannot work alone unless the other systems are in use. These other systems can be political, economic, social

and technological spheres as policymakers and implementers are still subjected to some conditions and factors, which could make or mar their policies. Like any other human inventions and reactions, the Actor-Network Theory has been faulted by scholars. One of the criticisms is that theory is largely descriptive and not explanatory, despite the criticisms; the significance of the theory in taking a holistic view of activities within our society cannot be over-emphasised. This theory suggests that attention should be given to human and non-human components in adopting an electronic-based innovation.

Another theoretical path of this work is the institutional theory of Philip Selznick (1957). Institutional theory is a product of intellectual journey of Philip Selznick. Selznick established institutional theory in 1957. The theory introduced institutional approach into the core field of administration that is, policy implementation. The theory exacts more influence on the adaptability of institutions to the environment where it operates. The theory illuminated on the fact that institution must design a method that takes into cognizance scarce resources, social support and institutional pressures in the process of implementing its strategies and tactics (Deephouse, 1996; Staw and Esptein, 2000; John et al, 2001). The strength of the theory lies in the belief that the institution will attain a near-perfect situation after several processes of similar nature have been carried out. Similarly, the theory assumes that for the organisation to be effective, attention must be paid to individual contributions in the organisation as well as the environmental pressure, which can limit present and future goals of an institution (Scott, 1985). According to Scott, the important ingredients to be considered in forming a working institution are the institutional integrity and continuity. He further observed organisation relation with the environment, informal relation within the institution, commonality and congruency of duties and roles of the organisation as other variables to be considered. Scott (1985) expanded the argument by stating, "institutional commitments develop over time as the organisation confronts external constraints and pressures from its environment as well as changes in the composition of its personnel, their interest, and their informal relations"

A succinct review of the historicity of institutional theory agreed that the theory derived its existence from sociological formulations and perspectives (Scott, 1987). Therefore, the body of works has been carried out to strengthen the tentacles of institutional theory. Hence, these submissions are premised on diverse thinking and views. Thus, institutionalisation is viewed as; the process of instilling value; the process of creating reality; distinct societal spheres; a class of elements. However, this study rest upon the view, which expresses institutionalisation as a way of promoting value in the society. Fundamentally, the argument here is that social orderliness is conceived as humanistic tendencies that are covered in social interaction. It is believed that social order exists through human actions and when these actions re-occur more often, it becomes structured and institutionalised (Berger and Luckmann, 1967). For instance, Berger, Berger, and Keller (1973) presented that modern awareness of society is modeled along series of interrelated systems that relate with advancement in (i) technological innovations (ii) rules and regulations (Bureaucracies) (iii) Multiplicity of real-life situations. This theory suggests that for any institution to be effective, concrete attention must be offered to external forces such as social, economic and political environments. The theory provides a theoretical explanation on how institutions exist to contribute to social orderliness in society. The theory identified a productive combination of available resources, social support and institutional pressure as a prerequisite for the organisation to survive. This

implies that for any public policy to be optimally implemented, the regulatory institution created to oversee the policy must be fashioned in a manner that resources(materials and human) available are well utilised, social implications are considered; pressure from other institutions (most often, of higher authority) are curtailed. Furthermore, the theory promoted an arrangement that should be followed perhaps when establishing the institution. It gives a framework that will aid the achievement of predetermined goals of any public institution. This includes interconnectedness of several structures that have technological, bureaucracy and multiple orientations undertones. Overall, the theory avails policymakers and administrators' ways to structure an institution in an optional manner with a view to achieving the predetermined policy objectives while giving the external environment the required attention.

METHODOLOGY

This work employed descriptive (qualitative and quantitative) research design as its blueprints. The study utilised a survey method to systematically seek data from the respondents using questionnaire and in-depth interview as research instruments. This study carried was out in the southwest geopolitical region in Nigeria. The south west was selected because it had the highest coverage (enrollment) for the period covered by this study. The region is densely populated by Yoruba speaking people and located along the West Africa Costliness, thereby having similar climatic condition, alternating dry and rainy season. The region comprises of six (6) states namely, Ekiti, Lagos, Ogun, Ondo, Osun and Oyo. The survey was conducted among the staff of National Identity Management Commission (NIMC), Nigerian Immigration Service (NIS) and Federal Road Safety Corps (FRSC) and Independent National Electoral Commission (INEC) in the selected three states (i.e. 50% of states in Southwestern Nigeria). NIMC was selected as the institution in the forefront of the policy implementation while NIS, FRSC and INEC were selected because of the currency and consistency of their activities in identity management. The study population was 2139; this included Ogun (766); Oyo (812); Ekiti (561). The National Identity Management Commission was selected being the regulatory agency in charge of the policy under review while Nigerian Immigration Service, Federal Road Safety Corps, and Independent National Electoral Commission were selected because of the currency and consistency of their activities in identity management.

The study employed multi-stage sampling technique. In the first stage, three states in the study area were selected using stratified sampling techniques from the three axes of Lagos/Ogun, Oyo/Osun, Ekiti/Ondo. Lagos/Ogun was grouped based on geographical proximity, Oyo/Osun was paired based on their common socio-political orientation, Ekiti/Ondo was combined based on common socio-political orientation. At the second stage, the National Identity Management Commission was purposefully selected being the institution in the forefront of the policy implementation, also, Nigerian Immigration Service, Federal Road Safety Corps, and Independent National Electoral Commission were purposefully selected because of the currency and consistency of their activities in identity management. The sample size of the study was 214 representing 10% of the study population (see Table 1)A well-structured questionnaire was administered to the selected staff of NIMC, NIS, FRSC and INEC on the constraints of the implementation of the national policy on identity management system in Southwestern Nigeria and these items

were measured using 4 ratings Likert scale of (1 – Not Significant, 2 – Slightly Significant, 3 – Averagely Significant, 4 – Highly Significant). The interview guide was administered on the interviewees in order to further gather information on the policy implementation. Deputy coordinator, one facility manager, enrollment officers from NIMC, public relation officers and two technical officers from NIS, FRSC and INEC were interviewed. They were interviewed because of their strategic positions in providing information on the issues affecting the implementation of the policy. Two hundred and fourteen (214) copies of questionnaire were administered to the respondents and two hundred and five (205) copies were retrieved. This means the response rate is over 90%. The quantitative data generated were subjected to descriptive statistical analysis while qualitative responses from participants in the interview conducted were logically narrated and reviewed in order to complement results from quantitative analysis.

Table 1 Population and sample

STATE	Number of Staff				Population e = (a + b +c+d)	Sample Size: (10% of e)
	Policy Implementers	Selected Government Agencies				
	NIMC (a)	NIS (b)	FRSC (c)	INEC (d)		
OGUN	110	303	286	67	766	77
OYO	122	312	306	72	812	81
EKITI	79	201	218	63	561	56
TOTAL					2139	214

Source: Pre-field Survey, 2019

DATA PRESENTATION AND ANALYSIS

Socio-demographics and Implications

This section presents the analysis and interpretations of relevant socio-demographical attributes of the respondents that participated in the survey. This was done in order to ascertain the relevance and predictability influence of personal features of the respondents on the results of the survey conducted. Table and percentages were used to analyse frequency of a feature of the respondents or the institutions while standard deviation reported the level of evenness in the distribution of respondents sampled for the study. A standard deviation that is less than one (i.e SD<1) indicates that the distribution tends towards equal representation while a standard deviation with a value greater than one (i.e SD >1) tends towards unequal representation. In terms of sex distribution of the respondents, Table 2 shows that out 135 male respondents, who participated in the survey 13.3% (18) were from NIMC, 41.5% (56) were from NIS, 34.8% (47) were from FRSC and 104% (14) were from INEC. 70 female respondents took part in the survey. These were distributed as follows: 14.3% (10) – NIMC; 22.9% (16)-NIS; 38.6% (27) – FRSC; 24.3% (17) – INEC. From this distribution, NIS had the highest number of male respondents in the survey while FRSC had highest number of female respondents. The mean value of 1.3 and standard deviation of 0.48 indicated that the distribution tended towards equal

representation, though a slight spread occurred between the categorical variables tested. This might be attributed to the nature of the activities of these agencies or deliberate policy directives of the government. Reviewing the age distribution of the respondents, analysis enumerated in the table revealed that on the overall basis, 10.7% (22) of respondents were between the ages of 20-30 yrs, 55.6% (114) were aged between 31-40yrs, and 15.6% (32) were aged between 51-60yrs. The spread indicated in the mean value of 2.4 and standard deviation of 0.88 shows that majority of the respondents fell within the age range of 31 to 41yrs. Therefore, it is assumed that the respondents are mature enough to express their independent view on the implementation of national policy on identity management system in the study area.

Respondents were also asked to indicate the number of years they had spent in their respective institutions. Overall, 14.6% (30) had worked for 5yrs and below, 13.2% (27) had worked for 6-10yrs, 25.9% (53) had worked for 11-15yrs, 21.5% (44) had also worked for between 16-20yrs of active service in their respective institutions. 11.7% (24) of the respondents had also worked for a period between 21 – 30yrs, 13.2% (27) of the respondents had worked for 31-35yrs as at the time the survey was conducted. It further displays respondents' years in service on institutional basis. The table revealed that respondents from NIMC had work experience not more than 15 years, this indicated that the agency responsible for implementation of the policy only existed for less than 15yrs. This is substantiated by a mean value of 3.3 and a standard deviation of 1.6. Summarily, it implies that over 67% of the respondents have had more than 10yrs experience in the identity management sector in Nigeria. As such, they are expected to provide reliable responses to items raised in the research instrument. This added more validity to the results generated by the study. On the basis of study location (state), the table enumerated that out of 74 respondents drafted from Ogun State, 13.5% (10) were from NIMC, 44.6% (33) were from NIS, 32.4% (24) came from FRSC and 9.5% (7) came from INEC staff in the state. Also, 79 respondents came from Oyo State of which 13.9% (11) came from NIMC, 32.9% (26) came from NIS, 39.2% (31) came from FRSC and 13.9%(11) came from INEC. From Ekiti state, 52 respondents were sampled, this included 13.5% (7) from NIMC, 25% (13) from NIS, 36.5% (19) from FRSC and 25% (13) from INEC. This result shows equal representation among selected institutions across the states with a mean value of 1.9 and a standard deviation of 0.78. This indicates that none of the respondents of the selected institutions was given biased representation in expressing their view on the construct of the study. In view of academic qualification of the respondents, only (22) of the respondents had secondary education while 89.3% (183) of the respondents were educated up to tertiary level. This was further subdivided across selected institutions as follows. Secondary education NIMC – 13.6% (3); NIS – 36.4%(8); FRSC- 36.4% (8); INEC – 13.6% (3) and tertiary education NIMC – 13.7% (25); NIS – 35% (64); FRSC – 36.1% (66); INEC-15.3% (28). This distribution produced a mean value of 2.9 and a standard deviation of 0.31. Largely, the composition of the respondents' shows that majority of them were educated enough and as such provided reliable and accurate information in terms of their knowledge of the new identity management regime in Nigeria.

Table 2 Socio-demographics analysis of the Respondents (N=205)

Socio-demographic	Response	Institution	Overall Total (%)

Variables			NIMC	NIS	FRSC	INEC	
Sex	Male	Freq.	18	56	47	14	135(65.9)
		%	13.3%	41.5%	34.8%	10.4%	
	Female	Freq.	10	16	27	17	70(34.1)
		%	14.3%	22.9%	38.6%	24.3%	
Age	20-30yrs	Freq.	2	9	9	2	22(10.7)
		%	9.1%	40.9%	40.9%	9.1%	
	31-40yrs	Freq.	18	36	38	22	114(55.6)
		%	15.8%	31.6%	33.3%	19.3%	
	41-50yrs	Freq.	5	14	15	3	37(18.0)
		%	13.5%	37.8%	40.5%	8.1%	
	51-60yrs	Freq.	3	13	12	4	32(15.6)
		%	9.4%	40.6%	37.5%	12.5%	
Education	Secondary	Freq.	3	8	8	3	22(10.7)
		%	13.6%	36.4%	36.4%	13.6%	
	Tertiary	Freq.	25	64	66	28	183(89.3)
		%	13.7%	35.0%	36.1%	15.3%	
Years in Service	Below 5yrs	Freq.	11	7	6	6	30(14.6)
		%	39.3%	9.7%	8.1%	19.4%	
	6-10yrs	Freq.	7	5	6	9	27(13.2)
		%	25.0%	6.9%	8.1%	29.0%	
	11-15yrs	Freq.	10	13	17	13	53(25.9)
		%	35.7%	18.1%	23.0%	41.9%	
	16 – 20yrs	Freq.	0	21	21	2	44(21.5)
		%	0.0%	29.2%	28.4%	6.5%	
	21 – 30yrs	Freq.	0	12	12	0	24(11.7)
		%	0.0%	16.7%	16.2%	0.0%	
	31-35yrs	Freq.	0	14	12	1	27(13.2)
		%	0.0%	19.4%	16.2%	3.2%	
Location (State)	Ogun	Freq.	10	33	24	7	74(36.1)

Source: Field Survey, 2019

CONSTRAINTS OF THE NATIONAL POLICY ON IDENTIFICATION IN NIGERIA

This section provides empirical results on challenges identified in the study as those confronting the implementation of national policy on identify management. A five-dimension rating scale was used to measure the perception of staff in the selected agencies

on the significance or otherwise of each of the challenges identified. The scale was sub-scaled into Highly Significant (3), Averagely Significant (2), Slightly Significant (1) and Not Significant (0). Mode statistics was used to infer the direction of responses on each of the identified challenges in Table 3. Sum Score (SS) and Relative Impact Index (Rll) were further computed in order to rank the challenges in the order of their impact on the implementation process. Item 1 in the research instrument tested institutional corrupt practices as a challenge to the policy implementation. The outcome of the analysis revealed that institutional corrupt practices is highly significant (50.2%) compared to other issues militating against the implementation of the policy under review. Institutional corruption was ranked 6th among challenges identified by the study with a sum score (456) and a RII (2.22). This implies that although institutional corruption qualified as a challenge to the implementation of the policy, it might not a critical factor to be considered. The privacy concern of the citizens were ranked 12th among the suggested challenges. This view was reported by 55.1% of the respondents that saw the privacy concerns of the citizens as slightly significant when compared with other factors foot-dragging the implementation of the policy. This result produced a sum score (241) and a RII (1.18). Insufficient central database infrastructure exerted highly significant influence (62.9%) on the implementation of the new identity regime. This factor was ranked as the leading challenge confronting the implementation of the policy with sum score a (494) and a RII (2.41). This is an indication that central database infrastructure is a major factor to be considered when re-working the implementation of the policy. Item 4 on the research instrument tested inadequacy of data protection measures as a clog in the policy implementation process. The result placed inadequate protection measures as a slightly significant challenge with sum score (282) and RII (1.38). Inadequate data protection was ranked 10th among the suggested constraints of the policy implementation. The inadequacy of data protection is a factor but seems not to be a pressing challenge that affects the execution of the policy being considered.

Limited human resources appeared to confront the implementation of the policy under review but in a slightly significant manner. This result came with sum score (245) and RII (1.20). It ranked 11th on the table and was supported by 68.3% of the respondents. 42% of the respondents claimed that limited public awareness exerted an averagely significant influence on the implementation. Though the result was not convincing enough, limited public awareness ranked 9th among the challenges tested in the research instrument. This concussion was supported by a sum score (351) and a RII (1.71). This implies that public awareness needs to be given adequate consideration in the process of the policy implementation. Another challenge that clogged the implementation of the policy was confirmed to be ineffective feedback process. This position was corroborated by 60.5% of the respondents. The result also attached a sum score (364) and a RII (1.78) to this variable which ranked 8th. This outcome portrayed that complaint and feedback process designed to monitor the implementation of the policy needs a revisit. This factor was rated to be averagely significant. Internet connectivity issue was reported to be the second leading challenge confronting the deployment of the new identity regime. This result came with sum score (493) and RII (2.40). The inability to provide strong internet connection might hamper the enrollment process as well as affect interaction with the new national database. This factor exerted a highly significant influence (63.9%) on the implementation process. Sixty-two per cent (62.4%) of the respondents pointed to unstable electricity as highly significant among other challenges confronting the implementation of the policy. This

outcome predicted the possibility of frequent down time and delay in the enrollment process which is an important element in the new regime being implemented. This issue ranked third among others with sum score (472) and RII (2.30). Insufficient enrollment and distribution centres (50.7%) as well as exclusion of vulnerable groups (47.8%) were tested as variables respectively. The two variables also produced sum score (231); (190) and RII (1.13); (0.93) respectively. This indicated that insufficient enrollment and distribution centres as well as exclusion of vulnerable groups did not constitute major bottlenecks in the implementation process of the new identity system in the study area as they ranked 13th and 14th. The issue of funding was raised by 55.6% of the respondent as a highly significant challenge faced in the process of implementing the policy under evaluation. This came in the 5th position among others with a sum score (460) and a RII (2.24).This result casted doubt on the financial provision made for the implementation of the policy by the government. Incomplete integration of functional databases into the national database manned by NIMC was averagely significant among challenges raised in the research instrument. 61.5% of the respondents attested to this with sum score (398) and RII (1.94). This item was ranked 7th among the others. The analysis revealed that integration of existing databases as directed in the policy document has failed to materialize. This means the implementation process is being truncated by this factor. The result shows that relevant agencies still progress in error due to lack of clear delegation of responsibilities. This inference was drawn from the outcome that 56% of the respondents affirmed that lack of clear delegation of responsibilities as a challenge exerted highly significant influence on the implementation process. This item was ranked 4th with a sum score (467) and a RII (2.28).

A closer review of narrations of most of the interviewees revealed the following challenges clogging the implementation of the policy. Challenges such as inadequate public awareness of the new identity regime, lack of political will, poor funding and investment in the programme by the government, corruption, uneven distribution of enrollment centres (exclusion of rural areas), too much emphasis on documents required for enrollment and delay in the production of the general multiple purpose card (GMPC) were summarised from interview commentaries among which are: “Even producing the GMPC (the card) alone has been very hard, Federal government has not taken this project with more seriousness” – An officer from NIS. “The project is capital intensive. It needs more money from government” – An officer from the NIS “There is need for more infrastructure in terms of enrollment facilities in the rural areas, though some are in the local government offices but if they are also available at the rural community a lot of people would have enrolled” – An officer from the INEC. “There should be publicity, there is low publicity, and people still confuse the old card with the new smart card. In fact, people are not even aware of something like this exist”– An officer from the NIS. “Government should invest more in the project because of the advantages. It will give government correct and current database and enhance provision of security” – An officer from FRSC. The issues of logistics and facilities were also identified by the interviewees. For instance, poor internet connection and fueling of generating sets were termed to be the reasons why some enrollment officers demanded for money from prospective enrollees, an act which is prohibited by the Nigeria Identity Management Commission. Other things which were common among the staff interviewed were lack of government support and insufficient funding. This position was captured in a statement made by one interviewee. He said “the

source of problems we face in implementing this programme were simply lack of political will of government and underfunding of the project".

Table 3 Constraints of the Policy Implementation

SN	Items identified	N	Mode (%)	SS	RII	Rank
1	Institutional corrupt practices	205	HS (50.2)	456	2.22	6th
2	Privacy concerns by the citizens	205	SS (55.1)	241	1.18	12th
3	Insufficient central database infrastructure	205	HS (62.9)	494	2.41	1st
4	Inadequate data protection measures	205	SS (65.4)	282	1.38	10th
5	Limited human resources	205	SS (68.3)	245	1.20	11th
6	Limited public awareness	205	AS (42.0)	351	1.71	9th
7	Ineffective feedback process	205	AS (60.5)	364	1.78	8th
8	Unstable internet connectivity	205	HS (63.9)	493	2.40	2nd
9	Unstable power supply	205	HS (62.4)	472	2.30	3rd
10	Insufficient enrollment and distribution centres	205	NS (50.7)	231	1.13	13th
11	Exclusion of vulnerable groups	205	NS (47.8)	190	0.93	14th
12	Insufficient funding	205	HS (55.6)	460	2.24	5th
13	Incomplete integration of functional databases into national database	205	AV (61.5)	398	1.94	7th
14	Lack of clear delegation of responsibilities among relevant agencies	205	HS (56.1)	467	2.28	4th

Source: Field Survey, 2019. Highly Significant (HS); Averagely Significant (AS); Slightly Significant (SS); Not Significant (NS). SS (Sum Score); RII (Relative Impact Index); N (Total Responses)

DISCUSSION OF FINDINGS

The study identified a number of challenges facing implementation of the policy. Insufficient central database infrastructure was identified. This means that the central database infrastructure that will house identity-related information of individuals that are being captured because of the policy implementation might not provide adequate capacity required for the policy to be effectively implemented. This was substantiated by Anderson *et al*. (2016) that delay in completion of central database infrastructure undermined implementation of identity systems in their case studies. This challenge posed a serious drawback in the process of implementing the e-identification system as the whole identity ecosystem depends on it. The study revealed that unstable internet connection hampered the implementation of the policy. This was supported by 63.9% of the respondents. This was also confirmed from the narrations of the interview conducted. Literature further established unstable internet connection as a bane confronting the implementation of the identification system – (Olaniyi, 2017; Anderson *et al*., 2017). The study revealed that unstable power supply (electricity) is another challenge. The argument is that given the poor state of the energy sector in Nigeria, the enrollment process that depends heavily on electronics such as computers and printers will be affected if alternative means are not provided.

Just like the position of Olaniyi (2017), Udunze (2015) and Zelezny (2012), lack of a clear legal framework and delegation of responsibilities among government agencies were identified as bottlenecks confronting the implementation of the new identity regime. Evidence in literature established the problem of multiple capturing by government agencies that is indication that the legal framework established for the identity industry in

Nigeria is unclear. This led to litigation involving NIMC and commercial banks. Section 27 of NIMC Act placed the commission in the sole position to regulate identity-related information or issues in Nigeria. Despite this, several agencies continued to disjointedly carryout separate identity enrollments. This cast doubt on the possibility of having one unique identification system in Nigeria. This current study also identified insufficient finding as another challenge being faced in the process of implementing the policy. This outcome received support from interview session sand responses gathered through questionnaire. The interviews constantly mentioned inadequate funding as one of the major challenges limiting successful implementation of the policy. It was claimed that due to lack of political will of the government, inadequate financial support for the project was received from government. Literature evidence from Jan (2006), Harbitz and Boekle – Guffrida (2009) suggested a lack of traditional funding from the government led to the demand of enrollment fees by National Database and Registration Authority in Pakistan and Registro Nacional de Identificacion Estado Civil in Peru. The challenge of funding appears to be a general issue in developing identity systems in most developing countries (the Carter Center, 2011; Gelb & Clark, 2013; Chiluga, 2015). Finally, for Nigeria to exploit the benefits of an electronic-oriented identification system in her quest to tackle the mountain of development issues, aggressive redevelopment of the policy and framework on identification system that reflect the existing political, social, economic and cultural values is the starting point of the government intervention.

CONCLUSION

The major summation from the survey is that the ongoing development of biometric-driven identification system requires constant reevaluation vis-à-vis the targeted outcome. Therefore, more research of it is expected to explore the emerging issues from the implementation of the policy. The findings of this work indicted institutional, operational and legal capacities of the coordinating agency, the National Identity Management Commission (NIMC). On institutional basis, government should reform the existing arrangements in terms of budgetary allocation to the identity industry as the incidence of dwindling resources predict lack of government will to develop a system that deepen the governability of the state. The fragility of the institutional processes, especially during enrollment, calls for upward of review of the internal control mechanisms to block incentives for official corruption of the field officers. Operational logistics according to this survey further revealed that the level of preparedness for the smooth implementation of the policy under review was not optimal. The deployment of the policy is been foot-drag by infrastructural deficit, unstable electricity without reliable alternative and epileptic internet connectivity which portrays possible downtime for enrollment process. This is evident in the identity gap being recorded in Nigeria as against the countries that started the same activity almost at identical time. Hence, concerted plan should be developed to rework the identified constraints, for instance, government could decentralised the enrollment process following the telecommunication industry model used in registering SIM cards by accrediting private firms for the enrollment exercise. This method has proved productive in countries like Indian and Indonesia. Another fundamental clog of the Nigerian foundational identity system is the growing numbers of government and private agencies collecting biometric data for supposedly identification in an apparent violation of

the policy regulating the National Identification Scheme. The legal landscape requires for standardising the system appears toothless or weak. The act establishing the NIMIC positioned it as the sole coordinator and regulator of system but other sister agencies like Nigeria Immigration Service (NIS), Independent National Electoral Commission (INEC) and host of other agencies even in the private sector have continued to enroll individual without working synergy to collaborate with the coordinating agency in developing a foundational database. This absence of clear demarcation of responsibilities of government agencies in the identity management sector threaten the nation object as embedded in the slogan 'enrolled once and be identified for life'. For the system to be unique and foundational as claimed in the policy thrust, the policy guidelines on harmonisation and integration of existing functional database need an accelerated implementation and a separate legal instrument.

REFERENCES

1. Anderson, C., Biscaye, P., Coney, S., Ho, E., Hutchinson, B., Neidhartdt, M. and Reynolds, T. (2016). *ICT Facts and Figures* 2016. International Telecommunications Union Retrieved from D/Statistics/Documents/facts/ICTFactsFigures2015.pdf.
2. Arora, A. (2008). The Story of Social Networking upon the Internet: The Real Game. Bright Hub.
3. Asian Development Bank (2016). Identity for Development for Asian and the Pacific. Mandaluyong City, Philippines.
4. Ayamba, I. A., & Ekanem, O. (2016). National Identity Management in Nigeria: Policy Dimensions and Implementation. *International Journal for Humanities and Social Science Studies*, *3*(1), 279-287.
5. Backhouse, J. (2006). Interoperability of identity and identity management systems. Datenschutz und Datensicherheit-DuD, 30(9), 568-570.
6. Backhouse, J., Hsu, C., and McDonnell, A. (2003). Toward public-key infrastructure interoperability. *Communications of the ACM*, 46(6), 98-100.
7. Berger, P. L. and Luckmann, T. (1967): *The social construction of reality: A treatise in the sociology of knowledge*. Garden City, New York: Anchor Books.
8. Brands, S. (2002a). *Secure Access Management: Trends, Drivers and Solutions*. *Information Security Technical Report*, 7(3), 81-94.
9. Brands, S. (2002a). Secure Access Management: Trends, Drivers and Solutions. *Information Security Technical Report, 7*(3), 81-94.
10. Callon, M. (1999). *Actor-Network Theory – The Market Test*. In Hassard, J & Law, J. (ed.) Actor-Network Theory and After. Oxford: Blackwell Publishers.
11. Cameron, K. (2006). The Laws of Identity. *Microsoft Web Services Technical Articles*, from http://msdn.microsoft.com/en-us/library/ms996456.aspx
12. Castro, D. (2011). *Explaining International Leadership: Electronic Identification Systems.* Information Technology and Innovation Foundation.
13. Chilunga, Z. (2015, June 23). Goodall adjust Malawi budget to K930bn: To meet Judiciary, Education demands. *Nyasa Times.*
14. Clarke, R. (1994). Human identification in information systems: Management challenges and public policy issues. *Information Technology & People*, *7*(4), 6-37. MCB UP Ltd.
15. Claub, S., and Kohntopp, M., (2001). Identity Management and its Support of multi-lateral Security. *Computer Network*, 37, 205 – 219.
16. Crompton, M. (2004). User-centric Identity Management: An Oxymoron or the Key to getting Identity Management right? *Information Policy*, 15(4), 291-297.
17. Deephouse, D. L. (1996). Does isomorphism legitimate? *Academy of Management Journal*, 39(4): 1024-1039.

18. Denhardt, J., V. and Denhart, R., B. (2007). *The New Public Service: Serving not Steering*. New York: ME Sharpe, Inc.
19. Ducastel, N. (2015). *International Comparison of e-ID Means*. PBLQ Report, Government of Netherlands.
20. Dunleavy, P., Margetts, H., Bastow, S., and J. Tinkler. (2006). "New Public Management Is Dead: Long Live Digital-Era Governance. *Journal of Public Administration Research the Theory*, 16 (3): 467-494.
21. Durand, A. (2003). Three Phases of Identity Infrastructure Adoption. Retrieved from http://discuss.andredurand.com/stories/storyReader$343.
22. Future of IDentity in the Information Society Project (2005) WP2, D2.1. *Inventory of Topics and Clusters*, 21 September 2005, available at http://www.fidis.net/resources/deliverables/identity-of-identity/#c1755
23. Gelb, A. and Clark, J. (2013). "Identification for Development: The Biometrics Revolution." Working Paper 315, Center for Global Development, Washington, DC.
24. Greenwood, D. (2007). *The context for Identity Management Architectures and Trust Models.* Paper presented at the OECD Workshop on Digital Identity Management, Trondheim.
25. Hartitz, M. and Boekle, B. (2009). Democratic Governance, Citizenship, and Legal Identity. Institutional Capacity and Finance Sector.
26. Hassard, J., Law, J., and Lee, N. (1999). Preface Organization: Special Issue on Actor Network Theory. 6 (3), 387-390.
27. Independent Centre for Privacy Protection (ICPP) and Studio Notarile Genghini (2003). Identity Management Systems (IMS): Identification and Comparison Study.
28. Kalvet, T. (2012). Innovation: A factor explaining e-government success in Estonia. *Electronic Government, 9*, 142-157.
29. Latour, B. (2005). *Reassembling the Social: An Introduction to Actor-Network Theory*. New York: Oxford University Press.
30. Law, J. (1992). Notes on the Theory of the Actor-Network: Ordering, Strategy, and Heterogeneity. *Systems Practice*, 5(4), 379-393.
31. Lips, M., and Pang, C. (2008). *Identity Management in Information Age Government Exploring Concepts, Definitions, Approaches and Solutions*. Victoria University of Wellington, Kelburn, New Zealand.
32. McKenzie, R., M. Crompton & C. Wallis (2008), Use Cases for Identity Management in E-Government, in: IEEE Security & Privacy, 51-57.
33. Millard, J., and Carpenter, G. (2014). Case study analysis report of online collaboration and networking tools for social innovation, a deliverable of the project: The theoretical, empirical and policy foundations for building social innovation in Europe (TEPSIE), European Commission-7th Framework Programme.
34. Naumman, I and Hogben, G. (2008). Privacy features of European eID card specifications. *Network Security, 8*, 9-13.
35. Neyland, D. (2006). Dismissed Content and Discontent: An Analysis of the Strategic Aspects of Actor-Network Theory. Science, Technology & Human Values 31 (1), 29-52.
36. Ogunbela, G. K. (2019). *Implementation of National Policy on Identity Management System in Southwestern Nigeria*. (Master Thesis, Obafemi Awolowo University, Ile-Ife)
37. Ojaide, C.L., (2010). *Information Flow in A Restructured Nigeria National Identification: Election and Census Fraud Solution*. M.Sc. Thesis, Blekinge Institute of Technology, Karlskrona, Sweden.
38. Olaniyi, E. O. (2017). The Role of National Electronic Identity Cards in Enhancing Public Service Effectiveness: The Nigerian Case. (Master's Thesis, Tallinn University of Technology, Estonia).
39. Scorer, A. (2007). Identity Directories and Databases. In Birch, D. (Ed.), *Digital Identity Management: Technological, Business and Social Implications*. Aldershot: Gower Press.
40. Selznick, P. (1957). *Leadership in administration*. New York: Harper & Row
41. The Carter Center. (2013). Voter Identification Requirements and Public International Law: An Examination of Africa and Latin America.Udunze, B. (2014). $55m biometric budget: CBN,
42. NIMC at war over control of BVN scheme. The Sun. Retrieved from <http://sunnewsonline.com/new/55m-biometric budget-cbn-nimc- atwar- over-control-of-bvn-scheme.

43. United Nation Development Index Survey (2016)
44. Vassil, K., Solvak, M., Vinkel, P., and Alvarez, R. M. (2016).The diffusion of internet voting. Usage pattern of internet voting on Estonia between 2005 and 2015. *Government Information Quarterly*, 1-7.
45. World Bank Digital Identity Toolkit (2014).
46. World Bank Group Country Assessment Report (2015).
47. Zelazny, F. (2012). The Evolution of India's UID Program: Lessons Learned and Implications for Other Developing Countries. CGD Policy Paper 008. Washington, D.C.