International Journal Multimedia and Image Processing (IJMIP), Volume 4, Issues 1/2, March/June 2014

Privacy, Security and Trust Issues Arising from Outsourcing PII Data Collection in Developing Nations

A case of Nigeria e-government services

Love Adedayo, Ron Ruhl
Information System Security Management
Concordia University College of Alberta
Edmonton, Canada

Abstract

Outsourcing of IT functions is increasingly used in many organizations in sub-Saharan Africa especially in the e-government services. Many factors are responsible for this including scarcity of competent government employees with the required technical expertise, desire for higher quality as well as ability to focus on organizations' core areas. However, there are several security challenges associated with this process. This paper identifies the security challenges associated with the outsourcing of personally identifiable information (PII) data collection processes in developing nations where there are no adequate or sufficient IT regulatory framework in place to protect PII. The paper offers recommendations for the protection of citizens' PII data collection by service provider based on the adoption of Global best practices.

1. Introduction

In today's global economy, outsourcing has become a very common phenomenon and many large organizations have outsourced some or all of their IT functions. Factors like lower costs, improved productivity, higher quality, higher customer satisfaction, time to market, and ability to focus on core areas are some of the benefits of outsourcing. However, there are equally many challenges and risks associated with IT outsourcing [1]. *IT Outsourcing* is as an act of delegating or transferring some or all of the IT related decision making rights, business processes, internal activities, and services to external providers, who develop, manage, and administer these activities in accordance with agreed upon deliverables, performance standards and outputs, as set forth in the contractual agreement between the parties involved [2]. Whenever, there is an outsourcing decision, there is an inherent risk associated with it. In addition, in any outsourcing service agreement, there are some hidden costs, unexpected outcomes, diminishing service levels, to name a few [3].

The value of Personally Identifiable Information (PII) is rapidly becoming comparable to the value of traditional financial assets and its during outsourced data collection process must therefore be considered important to forestall the risk of cybercrimes. As technological development increases and aspects of day-to-day operations involving PII are performed electronically, there had also been a considerable increase in cybercrime and part of this can start with identity theft. While identity theft can occur through a variety of means, unprotected electronic communications is a primary target and these have placed e-services at a higher risk of these attacks. The numerous regulations and directives that exist in different countries for the protection of PII data are often vague and offer wider latitude and less guidance for specific controls, as obtainable for other forms of information like the Primary Account Number (PAN) referred to by the PCI DSS for the payment card industry. Many countries have fashioned the local regulations guiding the protection of PII data towards the model obtainable in the European Union's Data Protection Directive, the Directive on Privacy and Electronic Communications (2002/58/EC) and the United Kingdom Data Protection Act 1998. However, Nigeria currently has no local regulation on data protection [4]. The electronic government system (e-government) which refers to the use of information technology by government agencies has the ability to transform relations with citizens, businesses and other arms of government; has as one of its aims improved interaction between government and citizens (G2C). Thus as most developing nations become more concerned about the welfare of their citizen's residing outside their country and how they can be accounted for during a crisis situation; Nigerian Embassies in various countries around the world has also considered this move a necessity for the Nigerian Citizens living abroad. As of July 2013, out of the ninety three different Nigerian Embassies / High Commissions in various countries around the world, nine have taken the initiative to conduct a citizen registration for Nigerians in these countries. To achieve this, they have seized the advantage of technology to capture the PII data of Nigerian

citizens in the respective countries through the on-line registration portal they provide. The exercise according to these embassies is aimed at establishing and effectively monitoring of the number and spread of Nigerian citizens across these countries, in order to assist them in the event of natural or man-made disasters, and also to build enough 'critical mass' to convince the Nigerian Government for the approval of absentee voting in times of election [5]. However, these PII data collection process had been outsourced to external service providers in seven out of the observed nine Nigerian embassies across the world, thus creating the potential risk of identity theft and other cyber threats to the citizens' PII information [5].

Similarly in recent times the Nigerian ministry of Communication Technology which is aimed at promoting the utilization of ICT to optimize the communication infrastructure in Nigeria has as part of their functions service delivery to the general public and is currently using the initiative of automated processes for possible online delivery [6]. This ministry's G2C initiative to drive the e-government services include informed citizenry initiative which uses the web and new media to improve the G2C engagement and drive efficiency in government. These the ministry planned to achieve by outsourcing the data collection processes for the purposes of Health Insurance; National Identity Management; Drivers' Licence records; Tax records and other e-services that require the collection of PII information. According to the ministry, the outsourcing process has as one of its objectives the creation of over a thousand job opportunities to the various service providers [6]. The ministry also planned the adoption of IT shared services to enhance productivity levels and efficiency in government processes and service delivery to the general public, with the aim of automating these processes and for possible online delivery through the one-stop government portal [6]. Unfortunately, while these benefits are clear in-principle, in practice most IT outsourcing processes and shared service implementations are mostly associated with additional security risks and also creates the potential risk of identity theft and other cyber threats to the citizens' PII data being outsourced for collection by the various service providers. This is because the services providers are not guided by any existing globally acceptable data protection regulatory framework to prevent the misuse of the collected data for malicious purposes as well as prevent cross-border data transfer for unintended purposes. Moreover, if the outsourcing contractor is operating in another country, the laws for PII and protection may be different in that country. Unless this is taken into account in the service agreement itself, these differences in laws may introduce even more risk.

In Nigeria, the National Information Technology Development Agency (NITDA) was established in 2001 with the main focus to fashion best practices policies that will enable effective and efficient usage of ICT facilities and infrastructures in the country [7]. This step by the government however was not all-inclusive as it lacks the required regulations for global best practices which have made online users' PII data as well as the outsourced data collection process vulnerable to the risk of identity theft. It is therefore crucial that e-government services in developing nations consider carefully the privacy and security implications of outsourcing the collection of PII data and provide the required regulatory framework for the protection of all these sensitive information. They also need strategies for managing the PII information risk profile through contractual or other means.

This paper does not address specific regulations for the privacy and security of PII data and neither does it deals with the processing of PII data within a web application as may have been discussed in other research work. It instead, provides a high-level overview of the security implications for outsourcing PII data collection in developing nations where there are no effective regulatory framework in place for the protection of such sensitive information. It thus presents as a recommendation, the adoption of a globally acceptable IT regulatory framework to guide the outsourcing of sensitive PII data collection by e-government services. The objectives of this research include: the evaluation of the existing guidelines that protect sensitive PII data; evaluation of the potential security risks associated with the outsourcing of PII data collection by some e-government services; evaluation of the potential threats to PII data in e-government IT shared-services; as well as recommend the adoption of adequate regulatory framework to guide the outsourcing of sensitive PII data collection. The scope of this study is limited to the outsourcing process in the Nigerian e-government services. The next section provides the review for the related research.

2. Related Works

2.1. Privacy regulations in e-government web services

Different schools of thought had described PII from different perspectives. Table 1 shows the description of PII as defined by the United States Government Accountability Office (GAO) [8] and by the National Institute of Standards and Technology (NIST) [9].

Table 1. Description of Personally Identifiable Information (PII)

GAO		NIST	
PII is Any information about an individual maintained by an agency, including:		PII include but not limited to:	
a	any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records.	a	Name, such as full name, maiden name, mother's maiden name, or alias.
b	any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.	b	Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer's identification number, or financial account or credit card number.
		c	Address information, such as street address or email address.
		d	Personal characteristics, including photographic image (especially of face or other identifying characteristics), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry).

Many countries like the UK, Canada and the USA have their local regulations guiding the protection of PII in various forms. Examples of such regulations include the UK Data Protection Act of 1998, which makes provisions for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information; The European Union Data Protection Directive (EUDPD) of 2002 requires that all EU members must adopt national regulations to standardize the protection of data privacy for citizens throughout the EU. There is also the Canadian Personal Information Protection and Electronics Document Act (PIPEDA) of 2011 which is an Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act of 1985 [10]. The EU Directive on Data Protection 95/46/EC ("Directive") was adopted in 1995 for the purpose of mandating data protection standards within the European community. It required all EU member states to enact, no later than October 25, 1998, national legislation giving effect to its provisions to protect individual citizens' rights to privacy and to prevent the unauthorized dissemination of its citizens' personal information both within and outside the EU. The Directive proposes comprehensive legislation encompassing all sectors of industry and all instances of collection and use of personal data. Specifically, the Directive protects "the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data".

The definition of "personal data" in the EU context, is broader than that found in Canada's PIPEDA [11] and include information relating to an identified or identifiable natural person who "can be identified, *directly or indirectly*, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". "Processing of personal data" is defined as any operation performed upon personal data "whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction" [11]. In essence, all personal data held must comply with the following principles:

- personal data must be processed fairly and lawfully, with disclosure of the controller of the data, and disclosure of the purpose for which it is being collected;
- personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
- personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- Personal data must be accurate and, where necessary kept up to date. Reasonable steps must be taken to ensure that inaccurate, misleading or incomplete data is erased or rectified;
- Personal data must be kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which data were collected or for which they are further processed. Member States are required to establish appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific purposes.

The Directive requires EU Member States to provide judicial remedies to any individual whose rights to data privacy are violated. It also requires that Member states adopt suitable measures to ensure

the implementation of and sanctions under the Directive; most Member states have consequently adopted specialized data protection authorities, similar to those found in this country [11]. All these reveal how these nations take into cognizance the impact of technological advancement on their regulations and how the citizens' PII data can be adequately protected. However, Nigeria currently seems to have no enforceable local regulation on the protection of PII [4] as well as its outsourced collection, but only a decree in the Nigerian Constitution which states that: "The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected" [12]. This is generally vague and does not address the protection of the PII data collection outsourced to IT service providers in the various sectors of the Nigerian e-government services.

Data protection statutes around the world vary widely in their scope, application and special considerations and most of the aforementioned jurisdictions have adopted, or are adopting, legal restrictions on international data transfers either generally, or on specific types of data. For example the European Union restricts the flow of personal information to jurisdictions lacking 'adequate data protection' and requires that data collectors obtain explicit consent to the transfer of 'sensitive personal information' [11]. In Canada, the province of British Columbia and Nova Scotia have also adopted legislation that restricts the trans-border flow of personal information collected by, or on behalf of, public agencies. The Treasury Board of Canada also has published guidelines for federal agencies which suggest that, wherever possible, federal databases containing sensitive personal information should be located in and only accessible from within Canada; and, that federal department should consider severing the flow of personal information to any foreign-linked service provider presented with a production order contrary to Canadian privacy law [11]. In addition, a growing number of domestic and foreign regulations have also adopted special rules for the management of financial, health and other 'sensitive' personal information.

A study [5] was carried out recently to reveal how some Nigerian e-government web services process citizens' PII in unsecured web environment without adequate security in place on those web portals or any globally acceptable regulatory framework for online personal data protection and thus exposing the sensitive information to the threat of identity theft. In another related research on balancing security and privacy in e-government services [13], a "trustworthy system" was advocated to complement the multiple technical nuances of security so as to provide privacy, security and trust in e-government web services. It was also recommended that when developing e-government infrastructures, consideration must be given to metrics, certification, standardization, governance and management, as well as international agreements on interoperability (including process interaction, definitions and meta-level standardization and technical interoperability). Additionally, the World Bank ICT Intervention Project in sub-Saharan Africa presents another pointer to the fact that there is urgent need for a globally acceptable regulatory framework in developing nations [14].

The bank has been working closely with over 30 countries in Sub-Saharan Africa to improve ICT connectivity. At the same time, they have also launched projects and programs that develop e-government applications and IT-enabled service industry. An example of this was the launching of a US$40 million project called e-Ghana in 2006, which aims to provide support for improving Ghana's competitiveness in the IT/IT-enabled services industries, including Business Process Outsourcing (BPO), as well as support for enhancing public service delivery through e-government. Activities under this project include setting up a high-speed, government-wide communications network connecting key ministries, departments and agencies; establishing a shared portal infrastructure for key agencies; and developing electronic applications for the priority revenue-generating agencies in the country. However despite all of these, the World Bank still recognises that having the right trade environment is the only way to facilitate the development of ICT. Likewise, ICT can foster, enable and facilitate trade and the relationship between trade and ICT can be viewed from three angles of: trade in ICT (e.g., international telephone calls), trade in services to which ICT is a critical input (e.g., outsourcing data entry or computer programming services), also ICT as a general facilitator of other types of trade (e.g. a farmer using text messaging to check export prices). These three angles are collectively referred to as "ICT-related service trade." Furthermore, in 2007, the World Bank conducted a series of studies and capacity building on ICT-related service trade for Eastern and Southern African countries (Trade in Information and Communication Services). The study found that some of the critical elements necessary for successful ICT trade ("ICT-competitiveness") are not sufficient. These elements include network infrastructure; an enabling policy, legal and regulatory framework environment; the education and training required to have a labor force with necessary ICT skills; use of ICT applications by businesses and government; and consumer awareness. The Bank is following up on this analytical work with projects in Ghana, Kenya, Nigeria and Rwanda to facilitate trade in ICT business, particularly in business process outsourcing (BPO). These projects include, among other things, support to industry associations, development of IT

Parks, partnerships with the industry to take up training of manpower, and support to investment promotion activities. More countries are likely to be added based on readiness of interested countries and effectiveness of these earlier programs [14].

Although several studies had been carried out on privacy protection, e-government security and the need for a trustworthy e-government services as well as on cross border outsourcing and IT shared services; this study is distinct in that it exposes the fact that PII data become more vulnerable to several risks of malicious uses including that of identity theft threat when their collection are outsourced to external service providers. It also addresses the urgency of the need for Nigeria to adopt globally acceptable best practices of structured guidelines for PII data protection in e-government services.

2.2. Data protection regulations in Nigeria

With the advances in automation of data, concerted efforts had been made by different countries of the world and some regional bodies like the EU, to develop comprehensive body of regulations on data protection. These have incorporated principles that regulate the collection, retention, processing, transmission and use of data in the respective regions [4], these principles however tend to be more general in nature by addressing only the infringement on personal privacy of the individuals' PII and it does not address more specifically, the processing of PII data over an unsecured network. In Nigeria, the data protection regulation can be found in the Nigerian constitution as well as in the "Freedom of Information Act (FOI), 2011 [15], both of which are very general and vague and do not address the processing of PII data within any network environment. Although there was a bill proposed by the Nigerian legislature in 2005 on the Computer Security and critical Information Protection seeking to outlaw cybercrimes in Nigeria, the bill was only passed for second reading in November 2012.[1] Although the implementation of e-government services has been in Nigeria for some time now, there is little evidence or research to suggest that a clear framework for the adoption of e-government is being followed [16]. In a recent study by Adeniyi [4] on the need for data protection regulation in Nigeria, concerns of identity theft danger was expressed in the light of the recent Subscriber Identity Module (SIM) card registration of mobile phone users in Nigeria. This concern was brought about when the Nigerian Communication Commission (NCC), mandated every mobile phone user to register their PII data with their various service providers in order to have a credible database of SIM card holders in Nigeria. However, this laudable directive by the NCC did not take into consideration the inherent danger to the security of citizens as they register their PII data in an environment not subject to PII data privacy regulations neither are there rules of security compliance by the service providers. Several factors militate against the effective deployment of e-government services in developing nations some of which include: rapid technological changes, digital divide as well as citizens' expectations and seamless services. In Nigeria a major factor affecting the effective implementation of e-government was that of lack of a clear framework for the adoption of e-government to be followed. As such, when citizens have to reveal their private information through this medium in an environment not subject to PII data privacy regulation, it becomes a source of great concern to them. Given that the government have a responsibility to maintain the trust of citizens, ensuring that the e-government initiatives keep pace with the expectations of society in this area, is very critical in building trust among citizens [17].

The privacy and security of citizens when they use government services is also a major challenge in Nigeria. Citizens are often faced with providing personal information online when interacting with government, hence the government owes a duty to guarantee the privacy and security of this information. As a result, it will be a step in the right direction if the government ensures the development and implementation of an adequate security and privacy policy for the protection of citizens' PII data in e-government web services.

2.3. E-readiness in developing nations and the dangers of IT outsourcing

E-government varies from one country to the other and governments around the world are at various stages of e-government readiness and implementation as indicated by the UN e-government readiness reports with the European countries generally taking the top spots [18]. Being e-ready involves having the necessary legal and regulatory framework available to support e-government and ensuring positive end user perspectives towards e-government and this can make citizens to embrace and be more willing to participate in e-government [18]. From the UN analysis on 'Regional Average of e-government readiness, [18] it was explicitly revealed that Europe is clearly ahead of all other regions and Africa is far behind in terms of e-government readiness. From figure1 below, it can be seen that Europe is clearly ahead of other regions and Africa is far behind in e-readiness and especially Nigeria can be classified as 'not e-ready' based on the measurement used to access the level of e-readiness.

[1] Daily Independent: available at: http://dailyindependentnig.com/2012/11/rep-passes-anti-cybercrime-bill-for-second-reading/

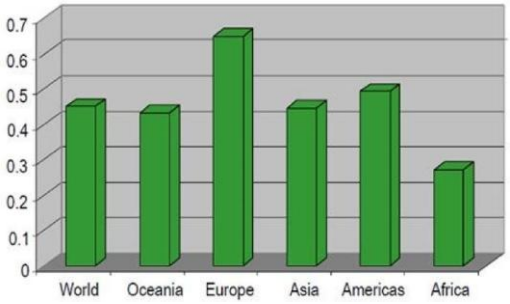

Figure 1. Differences in the e-Government readiness of different regions

Source: (UN, 2008) Regional average of e-Government readiness. [18].

The concerns about the dangers of outsourcing sensitive data across the borders of a nation was realized when in October 2003 in the United States a disgruntled Pakistani medical transcriber posted the medical records of several patients at the University of California, San Francisco (UCSF) on the Internet. Upset at the lack of payment for her services, the transcriber sought to force the issue by compromising the information [19]. The incident revealed that information sent offshore is prone to breach of confidentiality, that the obligations of those responsible for the integrity of the information are not well defined, and that consumers are not well informed of the potential problems or the actual incidents. The subjects of computer security and related law enforcement in India and Pakistan have been called into question, but the same issues can then be focused to other countries where work is likely to be outsourced and the subjects of computer security and law enforcement are equally questionable [19].

Recent incidents have reinvigorated the debate over issues of information privacy and confidentiality in several areas. Firstly, the efficacy of current American laws is under new scrutiny. Secondly, the gaps among the laws of the United States, the European Union, and countries popular for outsourced services have become prominent points of scrutiny. As a result, some American politicians have introduced new pieces of stringent legislation that provide clear guidelines, strict accountability, and penalties in order to keep such incidents from occurring. Some foreign countries lacking tough legislation are beginning to implement laws to meet American and European standards. If enacted, some recent proposed legislation will impose strict regulations regarding the confidentiality of information, especially with regard to information outsourced to a foreign country [19].

Even as concern about the amount of data being sent offshore has grown, several incidents involving the abuse of confidential, private information have continue to occur, fulfilling the worst fears of some consumers, legislators, and privacy experts. The incidents highlight the problems inherent in offshore outsourcing, the inability of U.S. laws to provide remedies, and the lack of procedural and technical controls by the parties outsourcing the data. In October 2003, Lubna Baloch, a Pakistani transcriber, threatened to post the medical records of several University of California San Francisco Medical Center (UCSF) patients on the Internet. The medical records had come into Baloch's possession by way of several American subcontractors [19].

In like manner, several offshore workers, based in Bangalore, India, employed by Heartland Information Services of Toledo, Ohio also threatened to expose confidential information unless they received a cash payment. This information had been extracted from training documents [19]. Similarly, in January of 2004, Wipro Spectramind, a New Delhi based telemarketing subcontractor for Capital One Financial Services, apparently lost its contract after an audit discovered that Wipro employees were, among other things, inflating credit terms available to customers[20]. Although a Wipro audit had characterized the problem as "unacceptable practices," it is clear that the employees were basing their actions on available customer credit information [20]. In each case, the status of the workers, either as a subcontractor or a direct employee, did not prevent the threat.

Considering the proliferation of these incidents in developed countries where are some form of regulations to protect their citizens' PII, It will therefore be imperative for developing nations especially Nigeria where there are no existing globally acceptable IT framework to protect the outsourced PII data collection to learn from these incidents and have a re-think on outsourcing the collection of citizens' PII data to service providers to avoid the unnecessary exposure of citizens' PII information to undue risks

3. Conclusion and Recommendation

The analysis of the e-government websites was analyzed to manually verify their outsourcing status without the use of any invasive mechanism. The process involves a non-invasive content analysis of the web sites by observing the page source and the page information of the respective websites from where the necessary parameters can be observed to determine the outsourcing status of the various websites. The findings of the research of data collection processes by the Nigerian Embassies reveals that the process of Outsourcing of the citizens' data collection was deployed by these embassies, thereby making the citizens to carry out the registration process in the web portal of the service providers on behalf of the various embassies. All of the embassies considered for the study except the Nigerian Embassy in Beijing China and Bern

Switzerland were found to have outsourced the registration processes; thus exposing citizens' PII to the attendant dangers of outsourcing such as fraud and identity theft. Table 2 gives the detailed urls of the various websites and their outsourced status.

IT outsourcing and shared services is fast becoming the easier alternative for most e-government services in developing nations among several other factors responsible for this is the requirement for highly skilled resources however the risks involved in these processes can sometimes be greater than the benefits being derived. The responsibility thus lies on the providers of e-government to ensure the privacy, security and trust of their citizens in the process of G2C interactions through the adoption of adequate regulatory framework that meets the standards of global best practice including managing the risks to PII in the service agreement and contractual processes.

Table 2. Outsourcing Status of the Embassies' Citizens' Registration Portal and Their URLs

COUNTRIES	OUTSOURCE	URLs
US1	**Y**	http://www.nigeria-consulate-atl.org/?page_id=88
US2	**Y**	http://www.nigeriahouse.com/RegistrationForm.aspx
CA	**Y**	http://www.nigeriahcottawa.ca/nhc2/index.php/en/welcome-to-nhc/citizens-registration/79-home/116-registration-form
FR	**Y**	http://www.nigeriafrance.com/page13.html
GE	**Y**	http://www.nigeriaembassygermany.org/registration.htm
SW	**N**	http://www.nigerianbern.org/
CH	**N**	http://www.nigeriaembassy.cn/register/
MA	**Y**	http://nigeria.org.my/index.php/consular/register
RU	**Y**	http://www.nigerianembassy.ru/nigerian-embassy-moscow?embnigeria=Consular%20Registration%20Form

US 1 = Atlanta Georgia, US 2 = New York, CA = Canada, FR = France, GE = Germany, SW = Switzerland, CH = China, MA = Malaysia, RU = Russia.

Although outsourcing generally has some benefits which include: cost efficiency, scalability as well as flexibility, there are a lot of inherent risks associated with outsourcing of citizens' PII data collection leading to dangers of the data being revealed to the service provider or any illegal user thus resulting in unexpected outcomes. Several risks on outsourcing business process operations had also been assessed to include a misuse of trust and security breaches [5] whereby the authors refers to a "misuse of trust" in a data privacy respect arguing that the external service provider needs access to non-encrypted sensitive data from the customers of a bank in order to process the outsourced transaction. Thus the risk is that service provider employees may use this data in an unauthorized manner (e.g. fraud or sale to competitors). In addition, none of the observed websites' registration portal has any form of spam protection against the potential vulnerability of the websites to server flooding as well as malicious users of the websites who can take advantage of this loophole to generate traffic to their own sites through the use of computer programs called 'bots' to automatically fill out web forms to create spam and these bots can generate spam much faster than a human can. These network attacks can threaten the stability of organizations' online services.

The first suggestion for mitigation will be the provision of adequate IT Security standard which will compel organizations deploying e-government services to comply with the required standards as provided by NIST and other globally acceptable best practices that address the protection of outsourced data collection process and cross-border data transfer. Another way to mitigate the cyber threats associated with outsourcing and IT shared-services is the adoption of a policy of strict access control with rule or role set based access privileges which use the need-to-know principle. These principles offer a greater degree of control on how the data will be processed in a safe environment. Only the administrator has the right to change security levels and these changes must be directed by the data owners (those in government responsible for the PII information). Similarly, ensure that when using outsourcing for the collection of citizens' PII that the tasks being outsourced follow stringent standards for the protection of the collected PII information and that the risk to loss of PII is identified, managed and also that the management of this risk becomes part of the service agreement itself.

4. Acknowledgements

My special appreciation goes to Professor Ron Ruhl of the Department of Information System Security Management, Concordia University College of Alberta for his immense support and encouragement throughout the course of writing this paper.

5. References

[1] Adeleye, B.C., Annansingh, F., Nunes, M.B, "Risk Management Practices in IS outsourcing: An investigation into commercial banks in Nigeria.," *International Journal of Information Management*, vol. 24, pp. 167-180, 2004.

[2] Dhar, S., Gangurde, R., & Sridar, R., "Global Information echnology Outsourcing: From a Risk Management Perspective.," in *5th Annual Global Information Technology World Conference*, San Diego, 2004.

[3] Aubert, B. A., Patry, M., Rivard, S., & Smith, H., "IT Outsourcing risk management at British petroleum," *Journal of Global Information Management,* vol. 14, no. 3, pp. 39-69, 2006

[4] A. Adeniyi, "The Need for Data Protection Law in Nigeria," 2012. [Online]. Available: http://adeadeniyi.wordpress.com/2012/07/18/the-need-for-data-protection-law-in-nigeria-2/.

[5] Love Adedayo, Ron Ruhl, Sergey Butakov & Dale Lindskog, "E-government Webservices and Security of Personally Identiable Information: A Case of Some Nigerian Embassies," in *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, London, 2013.

[6] Nigerian Ministry of Communication Technology," 2013. [Online]. Available: http://commtech.gov.ng/index.php/initiatives/e-government. [Accessed 20 January 2014].

[7] NITDA, "IT-Statistics," National Information Technology Development Agency, [Online]. Available: http://www.nitda.gov.ng/index.php/it-statistics. [Accessed 16 June 2013].

[8] "GAO Report 08-536, Privacy: Alternatives Exit for Enhancing Protection of Personally Identifiable Information," http://www.gao.gov/new.items/d08536.pdf, May 2008.

[9] NIST Special Publication 800-122: "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)", "National Institute of Standards and Technology," 2010. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf. [Accessed 20 5 2013].

[10] "Wikipedia," [Online]. Available: http://en.wikipedia.org/wiki/Information_security. [Accessed 16 June 2013].

[11] Jason, Young, "Privacy in IT Negotiation and Drafting", *Osgoode Professional Development CLE, Privacy and Data Security*, 2007.

[12] Nigerian Constitution, "Section 37 of the 1999 Nigerian Constitution," [Online]. Available: http://www.nigeria-law.org/ConstitutionOfTheFederalRepublicOfNigeria.htm. [Accessed 14 June 2013].

[13] Sullivan. K, Clarke. J, "Balancing Security and Privacy in e-Government Services IST-Africa," 2010. [Online]. Available: http://www.IST-Africaorg/Conference2010. [Accessed 5 June 2013].

[14] "Worldbank.org," [Online]. Available: http://live.worldbank.org/information-communications-technology-development. [Accessed 14 January 2014].

[15] Laws of the Federation of Nigeria, "Freedom of Information Act (FOI)," 2011. [Online]. Available: http://fmi.gov.ng/wp-content/uploads/2012/05/Freedom-Of-Information-Act.pdf. [Accessed 16 June 2013].

[16] "The Electronic Journal of E-Government," [Online]. Available: https://www.ejeg.com%2Fissue%2Fdownload.html%3FidArticle%3D205&ei=rZCuUZrvEsWcyQH0ioCYBA&usg=AFQjCNEOTUEJFjTIiSAR1wfkoGZ9ZMgbCw&bvm=bv.47380653,d.aWc. [Accessed 2 June 2013].

[17] Azenabor, C.E., Shoniregun, C.A., Imafidon, C., "e-Government Security Implications' Proceedings of Advances in Computing and Technology, (AC&T)," in *The School of Computing and Technology 4th Annual Conference*,, University of East London, 2009.

[18] Mundy, D and Musa, B. , "“Towards a Framework for eGovernment Development in Nigeria”," *Electronic Journal of E-Government,* vol. 8, no. 2, pp. 148-161, 2010.

[19] Lazarus, David "Extortion threat to patients' records. Clients not informed of India staff breach," San Francisco Chronicle, 2 April 2004. [Online]. Available: http://sfgate.com/cgi-bin/article.cgi?file=/c/a/2004/04/02/MNGI75VIEBI.DTL. [Accessed 15 Janary 2014]. "Capital one axes India call centre deal," Yahoo! Finance, March 2004. [Online]. Available: http://www.sfgate.com/egibin/article.cgi?file=/c/a/2003/10/22/MNGCO2FN8G1.DTL. [Accessed 28 December 2013].