Analysis of the Privacy Policies of Nigerian Online Shops

Olayiwola Wasiu Bello, Rafiat Ajibade Oyekunle and Rofiat Adeyemi

Department of Information and Communication Science

University of Ilorin

Email: laibello@gmail.com, ummusumayya1@yahoo.com and adeyemirofiat2@gmail.com

Abstract

Although privacy policies are posted by commerce websites to address privacy concerns of Internet shoppers including detailing their information practices on such policies, consumers seldom read and understand these policies. This study investigated privacy policy statements of 30 online shopping companies in Nigeria against the Fair Information Practice (FIP) principles. The privacy policy statements were examined and a checklist of 32 questions generated from the FIP principles was employed in carrying out the analysis. Findings from the study showed that most of the policies do not comply with the FIP principles entirely. The evaluated readability score (Flesch-Kincaid grade level, Flesch reading ease, the Gunning fog index and the SMOG readability formula), showed well above acceptable thresholds especially for public documents. However, majority of the policies showed proximity in terms of access as they can be reached through a single click from the landing page and contained how the information collected will be used. The study recommends that efforts should be made towards limiting the content and complexities of the policy statements using appropriate techniques and technologies and a regulatory body should be in place to review the privacy policy statements of online shops.

Keywords: Privacy policy, Online shops, Nigeria, websites, Consumers, Fair Information Practice

1. Introduction

The Internet has become a dominant medium of shopping associated with a growing sales volume online (Kim & Forsythe, 2010). Past, present and projected data available for global digital buyer penetration and e-commerce sales showed a continued rise (Statista[1,2], 2016). Local online shopping sector grew from 49.9 to 78 billion between 2010 and 2012 representing over 50% within 2 years (Euromonitor, 2014).

The marketplace opportunity presented by the information superhighway is growing at an exponential rate alongside other uses. Consequently, this has heightened the capacity and capabilities of business entities to accumulate, store, share, and analyse massive quantities of data emanating from transactions consummated by online consumers. This increase in data gathering and its use has raised the awareness of the public and consumer concerns in relation to online privacy (Wang and Wang, 2008). Likewise, concerns have been expressed about the infringements in relation to information privacy (Preibusch, 2013; Turow & Hennessy, 2007). Online privacy has thus become a key focus of consumer advocacy groups and policy makers (Federal Trade Commission [FTC] 2000), to promote consumer confidence as the new marketplace continue in its growth. Amongst the factors restricting the evolution of online shopping, security is considered the most important (Khaled, 2016; Uzun & Poturak, 2014). In order to boost e-commerce and its benefits for national economies, it is necessary to solve the online security problem (Khaled, 2016; Javadi, Dolatabad. Nourbakhsh, Poursaeedi. & Asadollahi, 2012; Hashim, Alam & Siraj, 2010). Other concerns include issues such as how information provided by online users could be used by marketers and security issues emanating from privacy factors, a main concern is the security of customers' personal identifiable information.

The retailing sector, with a strong boost from online shopping is growing, exceeding the rate of real GDP growth (Euromonitor, 2015). This is despite the fact that a sizable percentage of Internet users avoid online transactions as a result of their privacy and security concerns (Khaled, 2016; Uzun & Poturak, 2014; Lian & Lin, 2008) stemming from their unwillingness to send personal information over the Internet (Chakraborty, Lee, Bagchi-Sen, Upadhyaya, & Rao, 2016; Clemes, Gan, & Zhang, 2014; Roca, Garcia & De La Vega, 2009).

Transcending legal mandates, other factors drive the spread of privacy policies. Many businesses are encouraged by market pressure to, at the minimum, cast the notion of being sensitive to customers' privacy concerns. Most businesses would prefer to be distanced to the impression or insinuation that they aggregate and peddle the personal data obtained either openly or covertly from their customers to other entities (Nehf, 2005). As a matter of fact, it has become customary to see online service and product providers declare that they care about their consumers' privacy and clarify how data collected are used, stored and whether such data are shared with other parties. Websites include privacy policies to enlighten users on how their collected personal information is being used and/protected. However, these policies are sometimes usually difficult to comprehend, because they are usually verbose, take too long to read, and full of technical terms. This is despite users expressing growing concerns about information collection practices (Reidenberg, Travis, Lorrie, Cranor, & Brian, 2015) that form part of the issue the privacy policies are supposed to address.

It became necessary in the mid-1990s, for businesses that aggregated information from consumers in European during the course of any commercial obligations to circulate privacy policies in compliance with the European Union (EU) data protection guidelines (Nehf, 2005). For businesses of the United States of America (USA) origin, persuasive efforts of the Federal Trade Commission (FTC) which is an establishment of the Federal Trade Commission Act of 1914, played an influential role. Initiatives have also emanated from the African Continent Like the South Africa's Protection of Personal Information Act 4 of 2013, Ghana's Data Protection Act 2012 (Act 843), Mauritius' Data Protection Act 2004, Nigeria NITDA DRAFT GUIDELINES ON DATA PROTECTION 2013, among others. In the late 1990s, the FTC carried out studies relating to consumer privacy preferences and privacy practices of businesses (FTC, 2000) and these studies came to the conclusion that firms were profiting from the enormous amount of consumers' information in their custody without the consent or knowledge of the consumer. The information was also said to be used in ways that consumers had not approved of and by the nature of the internet, this problem was most acute. The reason is the ease at which personal information could be easily gathered, organized, and disseminated through a diversity of technological possibilities, of which consumers are not privy to (FTC, 2000). The disconnect between consumer considerations in relation to their privacy preferences and the practices of how businesses handle their data became grave by the end of the 1990s. This led the FTC to started the call for a national legislation towards fair information practice policies on the Internet. This resulted in the Fair Information Practice Principles (FIPP) of 1998 and the Children's Online Privacy Protection Act of 1998 alongside prior regulations like the Telemarketing and Consumer Fraud and Abuse Prevention Act of 1994. It is also important to capture studies by Council of Europe and the Organisation for Economic Co-operation and Development (OECD) in the late 1960's that was also instrumental to the recommendation that policy be developed to guard personal data in the custody of private and public sectors likewise. This effort gave birth to Convention for the Protection of Individuals in line with Automatic Processing of Personal Data (Convention 108) in 1981. Prior to this were the Swedish Data Act in 1973, West German Data Protection Act in 1977 and the French Law on Informatics, Data Banks and Freedoms in 1978 (Cavoukian, 1995).

The above are the foundation antecedents to the provision of privacy policies on websites to comply with the requirements of operational regulations. Therefore, the privacy policy statement of online shops should follow the requirements of the extant regulations, in order to indicate their honesty and grow more customers. Concerns for security has been raised in the literature with respect to online shopping or e-commerce in Nigeria. Aminu (2013) opined that security is one of the factors influencing the trend of online shopping adoption in Nigeria. This is similar to the findings of Ayo, Adewoye, & Oni (2011) and that of Akinyemi, Asani & Adigun (2013) that also found the

interrelationship between trust and perceived risk as a significant factor. These studies and others are mostly users' studies and focused on the acceptance, use and adoption of online shopping. These studies were carried out through a survey of users and determining which factors affect their desire for online shopping activity. In trying to extend the research focus on online shopping security concerns, the purpose of this paper is in threefold: firstly, to determine the accessibility of the privacy policies, to measure the readability of the privacy policy and lastly to investigate online shops websites' compliance with the FIP principles. By this, the approach in this study is that of providers' action towards compliance with provisions that could enhance trust and security of personal identifiable Information collected from the customers. This is important as customers feeling of insecurity as raised by other studies could be partly addressed through the proper implementation of the privacy policies.

2. Review of privacy principles and frameworks: Readability and Fair Information Practices

The Flesch Reading Ease (FRE) test is usually used to examine legal documents. FRE is based on a measure ranging from 0 to 100, where 0 corresponds to the most difficult to read document, and 100 indicates the peak of an easy to read document. In general, values from 60 to 100 are considered easy to read while 0-50 is considered difficult (Kincaid, Fishburne, Rogers, & Chissom, 1975). The Flesch Grade Level (FGL), Gunning fog and SMOG formula computes the number of schooling years required by an individual to be able to read and understand a statement. All are based on the Unites States of America educational system. Using FGL for example, a score of 9.0 means that a ninth grader (person with 9 years of education) would be able to understand a document. In Gunning fog, the "ideal" score is set at 7 or 8, anything above 12 is considered too complex for most people to read (Gunning, 1952). This ideal score is also common to FGL and the SMOG index (McLaughlin 1969). In fact, a lower threshold of 6 was recommended for public documents as presented in Doak, Doak, & Root (1996). There are a range of privacy principles articulated in various framework documents:

2.1 APEC Privacy Framework

The Asia-Pacific Economic Cooperation (APEC) Privacy Framework is closely related to other frameworks (Gerber, 2010) which are discussed in the following sections. This framework, focusses on real or possible that could arise through information disclosure, rather than the rights of individuals concerning their personal information. The OECD Privacy Principles is mainly supported within the EU and other governments' legal regimes, on the other hand, the APEC Privacy Framework is not supported by law. These frameworks major adopters have been global corporations, such as Apple Inc, IBM, Hewlett-Packard and lynda.com, Inc.

2.2 Generally Accepted Privacy Principles (GAPP)

The Generally Accepted Privacy Principles (GAPP) was developed by the American Institute of CPAs (AICPA) in association with the Canadian Institute of Chartered Accountants (CICA) in 2003 and was revised in the years 2006 and 2009. GAPP was developed having in mind business perspective. GAPP defined privacy as "the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information" (AICPA, 2009, p. 4). It is predicated on a mono privacy principle, being that the collection, usage, retention and disclosure of personally identifiable information must comply with the entity's privacy notice and with criteria set out in the GAPP as issued by the AICPA/CICA. It "operationalizes complex privacy requirements into a single privacy objective that is supported by 10 privacy principles. These principles are: management, notice, choice and consent, collection, use retention and disposal, access, disclosure to third parties, security for privacy, quality, monitoring and enforcement. Each principle is supported by objectives, measurable criteria that form the basis for effective management of privacy risk, and compliance requirements" (AICPA, 2009, p. 1).

2.3 OECD Privacy Principles

The OECD Privacy Principles could be adjudged as the most commonly used privacy framework especially because of its international acceptability and use. Its principle reflects the prevailing and developing privacy and data protection legislations from different countries and regions of the world, and provides the basis for the formation of foremost practices, privacy programmes and supplementary principles (Gerber, 2010). Over the past decade, OECD member countries have formulated laws for privacy protection, differing from country to country. The differences in laws may obstruct the free flow of information between countries, flows which has witnessed an increase in recent years with propensity to continue to grow as online transactions increases.

2.4 Fair Information Practice (FIP) Principles

The Federal Trade Commission is linked with the study of online privacy issues since 1995. The 2000 survey (FTC, 2000) demonstrated the insufficiency of industry efforts alone in this regard, drawing on evidence that self-regulatory initiatives are not broad-based implementation of effective self-regulatory programmes. The FIP Principles form the backbone of privacy laws in the United States as it forms the core of the Privacy Act of 1974 (Teufel, 2008). While the principles promoted by the FTC are only seen as guidelines, some state-level laws (e.g Privacy Act of 1974 Massachusetts Fair Information Practices 1975) have translated the guidelines into law (EPIC, 2016; ARN, 2016) and many businesses chose to develop trust relationship with their customers by safeguarding their privacy through self-regulation of the FIP Principles (CIPP Guide, 2016). The principles include: notice/awareness which states that individuals should be informed of an entity's privacy practices before the collection of personally identifiable information; choice/consent which states that individuals must have the right to agree or object to certain uses of their personal information; access/participation describes the ability of an individual to be able to view what data an entity has on record about him; integrity/security emphasises the accuracy of data, up-to-datedness, completeness and acceptable storage duration; enforcement/redress relates to the possibility of an individual to be able to seek redress against businesses. Furthermore, a mechanism should be put in place in place to oversee compliance with the set standards. This could be through a government regulation or self be self-promoted. The Fair Information Practice Principles are designed to direct how personal information are used in connection with business transactions. However, they are not enforceable legislations on their own (Gellman, 2015).

2.6 Related Studies: Privacy policies and FIPP

In a 2008 study, companies' privacy policy disclosures are reported to be signals to individuals about the fairness of their information practices, aimed at building trust and encouraging consumers to disclose their personal information (Boritz, Won, & Sundarraj, 2008). The result of the study showed a three-dimensional influence of the FIP principles on customers' privacy concerns. These are: information collection awareness, usage of information, and information sensitivity, but no concerns were however reported pertaining to the exchange of information for compensation and the relationships between businesses and online users. Earp, Anton, Aiman-Smith & Stufflebeam, (2005) investigated the difference between the information companies provided in their privacy policies and the information users are interested in about Internet privacy. The result showed that users' expectations are not being met by what companies addressed in their privacy policies. Whereas, the most frequently included item on privacy policies are consent to information collection, how data is collected and the security over collected data, and its transfer. However, users were most concerned about the type and use of their information collected, the transfer or sharing of their information and storage and maintenance of their personal information by organizations.

To develop a privacy policy interface that is more concise and user friendly, Chaianuchittrakul (2013) explored the potential of using crowd sourcing techniques to help improve usability and simplify complexity of privacy policies. The result showed that users think the context of a privacy policy is important and the users could understand privacy policies. Angelia (2014) designed and evaluated

some crowd-based techniques to minimise the time taken in reading privacy policies. Findings from the study suggested that privacy policies can be summarised by crowd-sourcing in conjunction with ranking method. Miller, Buck & Tygar (2012), introduced a metric to systematically analyse and evaluate a website's entire online privacy approach. Based on extant research, standards, and guidelines, Dehling, Gao, & Sunyaev (2014) designed and developed PPC – a privacy policy statement content assessment instrument to support the evaluation of the comprehensiveness of privacy policy content to address the concerns of users when it comes to their privacy. Their research was able to reveal the insufficient state of mHealth app privacy policy content. Becker, Jörg, Heddier, Marcel, Öksüz, Ayten, & Knackstedt (2014) through a laboratory experiment, investigated the effect of providing visualizations as means for communicating and security measures data privacy. The results indicated no significant effect on how users perceive their information security and privacy concerns with tis implementation.

Alhomod & Shafi (2013) examined the implementation of privacy policy in the educational sector of Saudi Arabia. Using data from a content analysis of the websites, by applying the FIPP, they opined that the study apart from providing an insight on the application of privacy policy in Saudi Arabia, could also help various stakeholders about their application of privacy policy in the country. Wurgler (2016) conducted a comprehensive empirical analysis using 261 privacy policies from seven different markets. The extent of compliance with the self-regulatory guidelines of FTC, US-EU Safe Harbor Agreement, and others were measured. The results suggested that privacy policies are being shaped impacted by market forces as well as by the different existing regulatory regime. From Africa, Kabanda, Brown, Nyamakura, & Keshav (2010) investigated the compliance of South African banks to the Electronic Communications and Transactions (ECT) Act No. 25 of 2002 which serves as a regulatory instrument concerning electronic communication transactions in South Africa. The findings indicated partial compliance with the ECT Act principles. Respondents were said to be fully unaware of all the ECT Act requirements and this is said to have implication on the banks' compliance. Also, Kelly (2013) investigated how to improve privacy notices in order to help consumers understand companies' data practices, the result showed that the standardized shorter labels were found to be helpful and more preferred by consumers.

Based on a threshold of sixth-grade level, Raj, Sharma Singh, and Goe (2016) evaluated 32 health information websites. Readability was assessed using Flesch Reading Ease Score (FRES), Flesch-Kincaid Grade Level (FKGL), and SMOG. Only about six websites were found to have readability scores at recommended sixth-grade level. With the goal of determining whether the accessibility and availability of privacy information affects individuals' purchasing decision, Tsai, Egelman, Cranor, and Acquisiti (2011) assessed the display of privacy policies of certain online shopping sites. The experiments showed that once privacy information is made more visible, people will tend to purchase from merchants that offer more privacy protection and even pay a premium to purchase from such merchants. To effectively ensure consumers find information in privacy policies Kelly, Cesca, Lucian, Bresee, Joanna & Cranor (2010) conducted an online user study of the nutrition label approach to enhance user understanding of privacy practices, increase the speed of information finding, and facilitate policy comparisons. The results of the study showed a significant impact of policy formats on the ability users to both quickly and accurately find information and on the attitude of users regarding their experience of using privacy policies. To address the problem of PPC (Privacy Policy Content) representation clarity, Mrosek (2015) looked at what aspects of the principles of information representation that already exist across different domains and how they work. The result contributed to the development of appropriate strategies for representing PPC. Lammel & Pek (2013) also used software language engineering methods to study usage profiles, correctness of policies, metrics, cloning and language extensions. The study concluded that the approach of Platform for Privacy Preferences Project's (P3P) to policy validation appears too weak to guarantee the correct use of the language.

3. Research Methodology: Exploratory survey of online shopping in Nigeria

Making use of content analysis, this study presents an exploratory survey of 30 online shops in Nigeria with the size purposively selected. As no known database of online shops was available, alexa.com (an international company that provides commercial web traffic data and analytics) was initially used to search for the online shops. However, the number of Nigerian shops available on alexa.com was limited, hence, a search on the World Wide Web (www) using the search word: Nigeria, online, shop store was conducted. Results were filtered to reflect only online shops of Nigerian origin with no international affiliation. Data was collected in the month of February, 2015.

Accessibility was evaluated from the perspectives of location and visibility. For readability, the analysis was carried out with the application of the Flesch-Kincaid grade level, Flesch reading ease, because of its convenience, and that it has been established to be valid and reliable (Paasche-Orlow, Taylor & Brancati 2003). However, Fitzsimmons, Michael, Hulley, & Scott (2010) are of the opinion that the Flesch-Kincaid formula underestimates reading difficulty significantly in comparison to the gold standard SMOG formula. As a result, SMOG and Gunning fog index was introduced to form a basis for comparison. The evaluation was done on a common online platform (readability-score.com) that has all the listed readability tests. A grade level of 8, as recommended by the original proponents of the tests was used as the difficulty threshold. Finally, a coding structure premised on the definitions of the five principles of FIP was carried out by reading the entire text and note of relevant occurrences manually.

Table 1: List of Investigated Online Shops

S/N	List of shops	Web address
1	Konga	http://www.konga.com.ng
2	Jumia	http://www.jumia.com.ng
3	Taafoo	http://www.taafoo.com
4	Buy am	http://www.buyam.com.ng
5	Buy Right	http://www.buyright.biz
6	Brand Nubians	http://www.brandnubians.com
7	Naija Styles	http://www.naijastyles.com
8	Outfit Galore	http://www.outfitgalore.com
9	Ostentation Clothing	http://www.ostentationclothing.com
10	Grand Products Company	http://www.grandproductscompany.com
11	Carmudi	http://www.carmudi.com.ng
12	Kaymu	http://www.kaymu.com.ng
13	Monster Bid	http://www.monsterbid.com
14	Osarmoire	http://www.osarmoire.com
15	My Store	http://www.mystore.com.ng
16	The London Plaza	http://www.thelondonplaza.com
17	Deal Dey	http://www.dealdey.com
18	Hello Food	http://www.hellofood.com.ng
19	Kara	http://www.kara.com.ng
20	Shopaholic	http://www.shopaholicng.com
21	Manna Stores	http://www.Mannastores.com
22	E London Stores	http://www.eLondonstores.com
23	Affordable Luxuries Online (ALO)	http://wwwAffordableluxuriesonline.com
24	Ozyet Collections	http://www.Ozyetcollections.com
25	Buy Correct	http://www.Buycorrect.com
26	Walahi	http://www.walahi.com
27	Ryte Deals	http://www.rytedeals.com
28	Pinky Bolar	http://www.pinkybolar.com
29	Shop and Mall	http://www.shopandmall.com.ng
30	Dress Rite	http://www.dressrite.biz

4. Results

4.1 Accessibility of Privacy Statement

In assessing how accessible the privacy policy statements in this study are, special emphasis was placed on where the privacy policy statements links were placed on the online shopping websites. It is expected that users are able to locate the privacy statement with relative ease. The accessibility assessment took a dual perspective: firstly, ease of locating the policy (existence of the policy link on the homepage); and secondly, how complete it is in accessing the policy (location of the link and its visibility). All the links on the sample examined contrast very well with the background and thus enhance visibility.

Table 2: Distribution of Privacy Policy Links on the Home Page

	Frequency	Percent
Sites without privacy policy links	1	3.3
Sites with privacy policy links	29	96.7
Total	30	100.0

Table 3: Distribution of Sites by Policy Link Position

	Frequency	Percent
Top	1	3.3
Middle	2	6.7
Bottom	27	90.0
Total	30	100.0

Table 2 shows that almost 97% offered a link on their homepage, while only one site (3.3%) did not offer a link on their home page, rather customers may have to go through the search button to get there. As links on home pages are created to access important web resource, this might be interpreted as a value of importance the providers place on it. Thus, most sites sampled in this study make the privacy policy link very accessible for their users. Similarly results on the evaluation of the link position on the home page presented in Table 3 shows that 90% of websites offered a link to the privacy policy from the bottom of the homepage, 6.7% offered a link in the middle of the page, while 3.3% offered a link at the top of the page. Links mostly placed at the top or bottom of pages stand out and easy to locate while those placed in the middle get clouded with other page resources. As menu items are mostly located at the top, items placed at the bottom are often easily located, as they tend to stand out. The examined online shops seem to conform to this design concept.

Table 4: Policy Links Isolated or Associated with other Links

	n	%
Isolated	1	3.3
Associated with other links	29	96.7
Total	30	100.0

Table 5: Privacy Policy Links accessed by a Single Click from the Homepage

	n	%
Policy accessed by a Single Click	29	96.7
Policy not accessed by a Single Click	1	3.3
Total	30	100.0

Working on the premise that a user might be on the shopping platform for a task and not having privacy policy in mind, it is assumed that placing the link among other frequently used resource could call the user's attention to the policy link. So the incidence of isolated policy links and incidence of links associated with other links was evaluated. Table 4 shows that for almost 97% of sites the privacy policy link is associated with other links, while only one site (3.3%) has a standalone privacy policy link. It is assumed that placing links with other links could enable users to locate such links, even when that was not the primary reason of activity on the site.

The number of click it takes to access the privacy policy from the home page was also examined. Table 5 shows that 29 (96.7%) sites have their policy link being accessed by a single click from the

home page and one site (3.3%) has its policy accessed by two clicks from the home page. The result here is encouraging as the more clicks it takes a user to get to a resource, the less likely they want to complete the process. Privacy policy statements within a single click saves users the trouble of going through many pages before getting to the policy page, which users finds easier than clicking through many pages. It was observed that all the sites examined have the privacy policy link available on all on all the pages collecting personal identifiable information (PII). Providing policy links on all pages collecting PII enables users to read the policy and makes them feel secure when they want to perform any transaction. To have access to the entire privacy policy document, it was observed that just a single click is required and the statements were not more than a single web page, though lengthy. As this minimises flipping through pages to access different section of the privacy policy, it has the propensity to encourage readership.

4.2 Readability of Privacy Statement

In evaluating the readability of the privacy policy statements, the size of the text in which the statements are presented was firstly examined.

Table 6: Frequency Distribution of Policy Text Font Size

Privacy Policy Font Text Size	Frequency	PERCENT
Size 10	0	0
Size 11	26	86.7
Size 12	4	13.3
> 12	0	0
Total	30	100.0

Table 6 shows that most of the sites are presented in font size '11' (86.7%) and some in size '12' (13.3%) with the font type for all in Times News Roman. For the sake of readability, font size '12' has been found adequate (Bernard, Mills, Peterson, & Storrer, 2001). However, the san serif Arial has been found to be more easy to read than the serif type face Times News Roman (Bernard, Lida, Riley, Hackler & Janzen, 2002). With the dominant size as '11' and in Times News Roman, the policy statements are considered to fall short of readability presentation standard.

The result of the readability sores is presented in Table 7. The mean FRES, FKGL, Gunning Fog and SMOG score of the online shopping websites were found to be 41.03, 12.54, 13.47 and 10.42 respectively (See table 8)

Table 7: Readability Scores

Readability scores	$N = 30$, n (%)
FRES	
Difficult (<50)	28(93.30)
Easy (>50)	2(6.70)
FKGL	
Up to grade 8	0(0)
Grades 9–10	0(0)
More than grade 10	30(100)
GUNNING FOG	
Up to grade 8	0(0)
Grades 9–10	6(20)
More than grade 10	24(80)
SMOG	
Up to grade 8	1(3.33)
Grades 9–10	13(46.70)
More than grade 10	16(53.30)

More than 90% (n=28) of the policy statement evaluated are difficult to read with FRES score (<50). It also turned out that none (0%) of the statements had FKGL and Gunning Fog readability score at eight-grade reading level. However, SMOG produced a 3.3% conformance with the eight-grade reading level. The result shows that most of the statements fall beyond the tenth-grade level which makes them to be considered as difficult to read. In comparing the results from the 3 grade level readability tests, Gunning Fog had higher values compared to the other two, with FKGL scoring the test higher than SMOG. While this result might point to the assertions of Fitzsimmons et al. (2010), the results compared to the threshold do not seem to have any significant difference. This is because, comparing the averages, all the test shows that the documents are difficult to read.

Table 8: Values of Readability Scores by its Average, Maximum, Minimum, and Range

	FRES	F-KGL	GUNNING FOG	SMOG
Average	41.03	12.54	13.47	10.42
Maximum	53.90	16.40	17.40	13.70
Minimum	26.70	10.50	9.70	8.00
Range	27.20	5.90	7.70	5.70

Variables which are used in computing the readability scores are presented in table 9. The number of words contained in the statements range from a maximum of 2757 to a minimum of 48, sentences from 132 to three while paragraphs are from 40 to 1.5. The average and maximum values of the number of words, sentence and paragraphs which are of course interrelated shows high values that tends to make the policy statements to be lengthy and possibly cumbersome to deal with, thereby potentially making most privacy statements hard for consumers to read and comprehend.

Table 9: Counts of the Readability Variables

Measures	Maximum	Minimum	Range	Average
Number of words	2805	48	2757	1309.87
Number of sentences	134	3	131	54.47
Number of paragraphs	64	2	62	27.73
Number of characters	14643	232	14411	6834.63
Number of syllables	4895	52	4843	1723.27
Sentences per paragraph	40	1.5	38.5	5.63
Words per sentence	29.6	15.3	14.3	21.55
Characters per words	5.4	4.6	0.8	5.00
Syllables per word	4.7	1.6	3.1	1.80
Passive sentence	42	0	42	14.40

4.3 Compliance with FIP Principles

The results indicate that all online shops in the survey sample (100%) posted a privacy policy, with some of the online shops stating the importance of customers reading their privacy policy. In this section, the specific concern of this study relates to the extent to which the online shops satisfied all five FIP principles.

Table 10: Personal Identifying Information

Policy Statements On PII	$N = 30$, n (%)
Type of PII Collected	
Not Mentioning	1(3.30)
Mentioning	29(96.70)
Purpose of Collecting PII	
Policies Specifying	30(100)

Table 10 shows that 29 (96.7%) policies mentioned the type of PII collected and only one (3.3%) policy did not mention the type of PII collected. It was also noted that all the online shops (100%) specified the purpose of collecting PII. Allowing users to know about the purpose and type of personal information being collected about them promotes transparency, could make customers feel safer and more secure about providing their personal information. Table 11 shows that 25 (83.33%) policies stated information about cookies while 5 (16.67%) did not state any information about cookies. Information on cookies usage gives some details of what information is being tracked by the cookies. For example, this could enable users to know that it does not contain any of their personal information but enables the browser to remember information specific to a given

Table 11: Cookies and Tracking Information

Policy Statements On Cookies and Tracking Information	N = 30, n (%)
Information about Cookies	
Policies Not Stating	5 (16.70)
Policies Stating	25(83.30)
Can Turn of Cookies	
Policies Not Stating	16 (53.30)
Policies Stating	14(46.70)
Tracking Information Collected	
Policies Not Telling	23(76.70)
Policies Telling	7(23.30)

As users should be at liberty to accept some conditions of website use, whether the online shops make provision for turning off cookies was evaluated. 14 policies (46.7%) tell users they can turn off cookies while 16 policies (53.3%) did not inform users they can turn off cookies. Informing users that they can turn off cookies will enable users to decide whether they want the browser to remember their information or not. With respect to tracking information collection, seven policies (23.3%) inform users that tracking information is collected while 23 policies (76.7%) did not inform users that tracking information is collected. If users have this information, it may make them more comfortable so that in the event of a fraudulent case, it might be easily detected and attended to.

Table 12: User Identification and Information Retention

Policy Statements On User Identification and Retention	N = 30, n (%)
Whether the Sites Identifies Users	
Policies Not Stating	22(73.33)
Policies Stating	8(26.67)
How Sites Identify Users	
IP address only	4(13.33)
Username and password	1(3.33)
IP address and password	1(3.33)
Password only	1(3.33)
IP address and ISP	1(3.33)
Retention Policy about Users	
Not stating	1(3.33)
Retaining all information	27(90.0)
Retaining some information	1(3.33)
Retaining some information	1(3.33)

Virtually all the online shops (90%) have it stated that they retain all information a user makes available while the rest retain only some of the information. The amount of information retained has implication for security as this could be used for other purposes. This however, puts the burden of securing such information on the online shops.

Table 13 shows that four policies (13.3%) make statements about sharing information with subsidiaries, one policy (3.3%) states that the online shop does not share any information, 15 policies (50%) state that the shops share some information, six of the policies (20%) state that the shops share

information only under legal obligation, one policy (3.3%) states that the shop shares information with third parties, two policies (6.7%) stated that the online shops share some of the information and only under legal obligation, while one policy (3.3%) states that there is no restriction to information sharing with subsidiaries. This shows that online shops do protect the privacy of their users to a limited extent, particularly from being made public, but not with respect to subsidiaries.

Table 13: Information Sharing with Subsidiaries

`	N=30	%
Policies sharing information with its subsidiaries	4	13.3
Policies not sharing any information	1	3.3
Polices sharing some of the information	15	50.0
Policies sharing information only under legal obligation	6	20.0
Policies sharing with third parties	1	3.3
Policies sharing some of the information and only under legal obligation	2	6.7
Policies not restricting information with its subsidiaries	1	3.3
Total	30	100

In Table 14, eight policies (26.7%) stated that the company will trade or sell user's personal information while 22 policies (73.3%) claimed not to trade or sell user's personal information. The policies stating that the company will sell user's personal information will sell only under legal obligation or business transfer.

Table 14: Use of Information Collected

Policy Statements On Information Use	N = 30, n (%)
Trade or Sell User's Personal Information	
Policies Not Stating	22(73.33)
Policies Stating	8(26.67)
Information used for Site Improvement	
Policies Not Stating	18(60.00)
Policies Stating	12(40.00)
User Profile Customization	
Policies Not Stating	22(73.33)
Policies Stating	8(26.67)
To Deliver Emails	
Policies Not Stating	3(10.00)
Policies Stating	27(90.00)
Sending Marketing Information to Users	
Policies Not Stating	3(710.00)
Policies Stating	27(70.00)

Some of the sites (12, 40%) use the information collected towards site improvement, eight policies (26.67%) claimed to use the information for user profile customization, while 27 (90%) stated that information gathered is used to deliver emails. Based on the user's information collected, sites do use the information in improving their sites. Some online shops do send emails occasionally informing customers about special offers, new products or other information which might interest users.

5. Analytical Discussion: Accessibility, Literacy and FIIP Guidelines

Online related transactions are gaining prominence in Nigeria as evidenced by its adoption by major service providers and proliferation of online shops. This could be partly due to improvement in telecommunication service and increased internet penetration. It can be said that online shoppers in Nigeria cuts across different age category and academic background and most of them must have been using other internet-based services. Searching for information on privacy policy is not likely to constitute much of a problem to them as this survey revealed that adequate measures were taken by the online shops in terms of making the policies accessible. These measures include making links to

the policies available conspicuously on the home page with minimal click to reach the document itself. This can also be considered a commitment to customer privacy on the part of the online shops.

A country´s literacy as described by the World Bank relates to the population including citizens starting from age 15 who can, read and write simple statement of their daily lives, with understanding. Sadly, almost 75% of the global illiterate adults originate from only ten countries which includes Nigeria in the top half (Indexmundi, 2015). From the global perspective and citing the Internet Society's Global Internet User Survey, privacy policies are read by only 16% of internet users. Out of this, only one-fifth actually understand them (ISOC, 2012). While illiteracy could be a factor in the low percentage in the reading of the policies, its complexities and difficulty to understand could just be the main contributory factor to this. This is indicated in the survey result presenting virtually all the policies being well above acceptable thresholds for readability especially for public documents.
Although many Internet users have preference for online transactions, they are inhibited by the risks relating to privacy and security issues as observed in the literature. To allay their fears, privacy policy statements are used by online shops and other online organisations to show their commitment to fair practice in the use and management of information collected from the shoppers. This is directed towards the protection of their customers' personal information from being used illegitimately, traded or shared with other entities without the consent of the individuals. Despite this, the policies go ahead in stating that information will be shared with subsidiaries and even in some cases with third parties, which could be a grave concern to the shopper. The concept of consent as required in the FIP principle is also another area for concern as this requires that the online shops to expressly request from the customer before their information is shared. Unfortunately, the shops only state that, they could share it and this does not literally translate to consent. While it might be near impossible to ask every customer at every time his information is going to be shared, a provision in the policy that allows for a yes or no to information sharing might just suffice. The ability of users to ask for information about what information an online shop has collected about them is a provision of the FIPP. However, none of the platform provided a vista to actualise this. This leaves the user with the option of sending a general mail to the shops for this and experimentation on this yielded no response.

While enforcement is part of the recommendation of the principles, this is basically in terms of the online shops or other service providers adhering to the requirements of the principles. Provisions for such are enshrined within the legal instruments in different countries as it relates to privacy issue. A perusal of the legal provisions in Nigeria, shows no one comprehensive data privacy or personal information protection law, with comprehensive provisions is available on the protection of citizens privacy (Akinsuyi, 2015; Udoma & Belo-Osagie, 2015). This is apart from Section 37 of the Nigerian Constitution (1999) which provides that; "The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected" (CFRN, 2004, Chapter C23, Section 37). However, the National Information Technology Development Agency (NITDA) have issued guidelines on data protection which are sadly not also enforceable.

6. Conclusion and Recommendations

This study investigated the commitment of online shops in Nigeria towards privacy concerns of the shoppers. The online shopping platforms were assessed based on accessibility, readability and compliance to the FIIP guidelines. The survey showed the online shops posted privacy statement on their website, with a relatively high accessibility standard. However, the complexity and verbose nature of the policy statements has implication for the ability of the users to read and possibly comprehend the information contained therein. Efforts should be made towards limiting the content and complexities of the policy statements. This could be done by using crowd-based techniques as suggested by Angelia (2014) or through the use of visualisations as posited by Becker, et al. (2014). By doing this, users might be better positioned to read and understand the policy statements and minimise their security concerns. A partial compliance with FIP was also observed, which could compromise the security of customer’s personal information. From the observations above, this study concludes that the privacy policy statements of online shops as currently provide, is not positioned to

adequately protect users' privacy rights. Furthermore, the online shops may be in practices of facilitating consumers' data collection by third parties, email spamming to users, or sharing email addresses with their affiliates. From the design perspective it is important to place privacy policy statement at one click of users to facilitate easy viewing. Online shops could also consider privacy seals which represent a stamp of approval demonstrating good privacy practice and high level of data protection compliance etiquettes and standards. Privacy seals are designed to be online branded trust mark or seal of approval emblem, which are commonly used by third party site verification services. They are integrated to protect online customers by identifying verified web sites with demonstrable services for the protection of the safety and online privacy of customers. This could further reduce the perceived fear the shoppers nurture. While a law on privacy related issue is still in the pipeline, there is a need for privacy policy statements of the online shops to be reviewed by a regulatory body. This will promote compliance with the laws as well as stipulated guidelines. Future research could look at other sectors associated with online transaction and user view specifically on their interaction with privacy policies.

REFERENCES

AICPA. (2009). Generally Accepted Privacy Principles. Retrieved from https://www.cpacanada.ca/-/media/site/operational/ms-member-services/docs/00250-generally-accepted-privacy-principles.pdf?la=en

Akinsuyi, F. F. (2015) Data Protection and Privacy Laws Nigeria, a Trillion Dollar Opportunity!!. Available at SSRN: http://ssrn.com/abstract=2598603 or http://dx.doi.org/10.2139/ssrn.2598603

Akinyemi I. O., Asani E. O., Adigun A . A. (2013). An Investigation of Users' Acceptance and Satisfaction of E-Banking System as a Panacea towards a Cashless Economy in Nigeria. Journal of Emerging Trends in Computing and Information Sciences Vol. 4, No.12 December 2013 Pp. 954-963

Alhomod, S. & Mudasir S. M. (2013). A study on implementation of privacy policy in educational sector websites in Saudi Arabia. global journal of computer science and technology network, web and security, 1-5. retrieved from htts://globaljournals.org

Aminu, S. A. (2013) Challenges Militating against Adoption of Online Shopping in Retail Industry in Nigeria. Journal of Marketing Management, 1(1), pp. 23-33.

Angelia. (2014). Crowd Verify: Using the Crowd to summarize website privacy policies (Unpublished master's thesis). Carnegie Mellon University Pittsburgh, PA U. S. A. Retrieved from http://cmuchimps.org/uploads/publication/paper/155/crowdverify_using_the_crowd_to_summarize_web_site_privacy_policies.pdf

Ayo, C. K., Adewoye, J. O., & Oni, A. A. (2011). Business-to-consumer e-commerce in Nigeria: Prospects and challenges. African Journal of Business Management, 5(13), 5109-5117.

Becker, J., Heddier, M., Öksüz, A., & Knackstedt, R. (2014). The Effect of Providing Visualizations in Privacy Policies on Trust in Data Privacy and Security. Paper presented at the Proceedings of the 47th Hawaii International Conference on System Sciences (HICSS '14), Waikoloa, Hawaii. retrieve from ieeexplore.ieee.org/xpls/abs_all.js

Bernard, M., Lida, B., Riley, S., Hackler, T. & Janzen, K. (2002). A Comparison of Popular Online Fonts: Which Size and Type is Best? Usability News, 4. 1. [Online]. Accessed 3/6/2016 from http://usabilitynews.org/a-comparison-of-popular-online-fonts-which-size-and-type-is-best/

Bernard, M., Mills, M., Peterson, M., & Storrer, K. (2001). A comparison of popular online fonts: Which are best and when? Usability News, 3. 2. [Online]. Accessed 3/6/2016 from http://usabilitynews.org/a-comparison-of-popular-online-fonts-which-is-best-and-when/

Boritz, E., Won, G. N. & Sundarraj, R. P. (2008). Do companies' online privacy policy disclosures match customer needs? Retrieved from *http://accounting.uwaterloo.ca/uwcisa/resources/eprivacy/Privacy%20Gap%202008-04-18.pdf*

Brad M., Buck K., and Tygar. J.D. (2012). Systematic analysis and evaluation of web privacy policies and implementations. The 7th International Conference for Internet Technology and Secure Transactions, (pp. 534-540). retrieved from www.cs.berkely.edu

Cavoukian, A. (1995). Who Knows: Safeguarding Your Privacy in A Networked World. Random House of Canada: Random House of Canada. ISBN 0-394-22472-8.

CFRN (2004). Constitution of the Federal Republic of Nigeria (Promulgation) Act, Chapter C23, Laws of the Federation of Nigeria 2004 (as amended)

Chaianuchittrakul, C. (2013) "Crowdsourcing privacy policy analysis: Evaluating the comfort, readability and importance of privacy policies," Ph.D. dissertation, Carnegie Mellon University, 2013. Retrieved from cmuchimps.org/../pub_download

Chakraborty R., Lee J., Bagchi-Sen S., Upadhyaya, S., Rao, H. R. (2016). Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. Decision Support Systems 83 (2016) 47–56

CIPP Guide (2016). Fair Information Practice Principles. Available at:https://www.cippguide.org/2010/01/18/fair-information- practices-principles/

Clemes M. D., Gan C., Zhang J. (2014). An empirical analysis of online shopping adoption in Beijing, China. Journal of Retailing and Consumer Services 21 (2014) 364–375

Dehling, T., Gao, F., and Ali, S. (2014). Assessment instrument for privacy policy content: Design and Evaluation of PPC. WISP 2014 Proceedings. retrieved from https://aisel.aisnet.org/wisp2014/2

Doak, C. C., Doak L., and Root, J. H. (1996). Teaching Patients with Low Literacy Skills, J. B. Lippincott, Philadelphia, Pa, USA, 2nd edition, 1996.

Earp, J. B., Anton, A. I., Aiman-Smith, L. & Stufflebeam, W. H. (2005). Examining Internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management* 52 (2), 227-237.

Euromonitor (2014) Online Shopping Report July. Accessed 24/5/2016 from http://www.phillipsconsulting.net/files/online_shopping_report.pdf

Euromonitor (2015) Retailing in Nigeria. Accessed 24/5/2016 from http://www.euromonitor.com/retailing-in-nigeria/report

Fitzsimmons, P.; Michael, B.; Hulley, J.; Scott, G. (2010). "A readability assessment of online Parkinson's disease information". J R Coll Physicians Edinb 40 (4): 292–6. doi:10.4997/JRCPE.2010.401. PMID 21132132.

FTC. (2000). Privacy online: Fair information practices in the electronic marketplace. Retrieved from http://www.ftc.gov/reports/privacy2000/privacy2000.pdf

Gellman, R. (2015). Fair Information Practices: A Basic History. Retrieved from http://bobgellman.com/rgdocs/rg-FIPShistory.pdf

Gerber, B. (2010). OECD Privacy Principles. Retrieved from http://oecdprivacy.org/#apec

Gunning, Robert (1952). The Technique of Clear Writing. McGraw-Hill. pp. 36–37

Hashim, F., Alam, G. M. & Siraj, S. (2010). e-Management for administrative efficiency in higher education through participatory decision-making. *WSEAS Transaction on Commununication*, *2*(9), 73-82.
http://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/

Indexmundi (2015). World Literacy Demographics. Retrieved 12/6/2016 from http://www.indexmundi.com/world/literacy.html

ISOC (2012). Global Internet User Survey, 2012. Retrieved 8/6/2016 from https://www.internetsociety.org/sites/default/files/rep-GIUS2012global-201211-en.pdf

Javadi . H. M., Dolatabadi H. R., Nourbakhsh, M., Poursaeedi,A. & Asadollahi A. R. (2012). An Analysis of Factors Affecting on Online Shopping Behavior of Consumers. International Journal of Marketing Studies; Vol. 4, No. 5; 2012 Pp. 81-98

Kabanda, S.K., Brown, I., Nyamakura, V. & Keshav, J., (2010). 'South African banks and their online privacy policy statements: A content analysis', SA Journal of Information Management 12(1), Art. #418, 7 pages. DOI:10.4102/sajim.v12i1.418

Kelley.P.G., "Conducting usable privacy & security studies with amazon's mechanical turk," in Symposium on Usable Privacy and Security(SOUPS) (Redmond, WA. Citeseer, 2010. Retrieved from http://doi.acm.org/10.1145/1753326.1753561

Kelley, P. G., Cesca, L., Bresee, J., & Cranor. L. F. (2010). Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach. Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10), Atlanta, Georgia, USA. retrieved from http:///repository.cmu.edu/files/pfs/tech_reports

Kelly, P. G. (2013). Designing privacy notices: Supporting user understanding and control,"Ph.D. dissertation, Carnegie Mellon University. Retrieved from repository.cmu.edu/cgi/viewcontent

Khaled M. S. F. (2016). An empirical analysis of factors predicting the behavioral intention to adopt Internet shopping technology among non-shoppers in a developing country context: Does gender matter? Journal of Retailing and Consumer Services 30 (2016) 140–164

Kim, J. & Forsythe, S., (2010). Factors affecting adoption of product virtualization technology for online consumer electronics shopping. *International Journal of Retail & Distribution Management*, *38*(3), 190-204.

Kincaid J. P., Fishburne R. P. Jr, Rogers R. L., & Chissom B. S. (February 1975). "Derivation of new readability formulas (Automated Readability Index, Fog Count and Flesch Reading Ease Formula) for

Navy enlisted personnel" (PDF). Research Branch Report 8-75, Millington, TN: Naval Technical Training, U. S. Naval Air Station, Memphis, TN. Accessed 4/6/2016 from http://www.dtic.mil/dtic/tr/fulltext/u2/a006655.pdf

Lian, J. & Lin, T., (2008). Effects of consumer characteristics on their acceptance of online shopping: Comparisons among different product types. *Computers in Human Behavior*, 24, 48 – 65.

McLaughlin, G. (1969). SMOG grading: A new readability formula. Journal of Reading, 12 (8). 639-646.

Mrosek, R. (2015). Representation of privacy policy content: a systematic literature review. Unpublished master's thesis, University of Cologne, Cologne. retrieved from www.isq.uni-koeln.e

Nehf, J. P. (2005). Shopping for privacy online: Consumer decision-making strategies and the emerging market for information privacy. *Journal of Law, Technology & Policy*. *5*(2), 1-54. Retrieved from http://illinoisjltp.com/journal/wp-content/uploads/2013/10/nehf.pdf

Paasche-Orlow, M.K., Taylor, H.A. & Brancati, F.L., 2003, 'Readability standards for informed-consent forms as compared with actual readability', New England Journal of Medicine, 348(8).

Preibusch, S. (2013). Guide to measuring privacy concern: Review of survey and observational instruments International Journal of Human-Computer Studies, 71(12), 1133-1143

Raj, S., Sharma, V. L., Singh, A.J. and Goe, S. (2016). Evaluation of Quality and Readability of Health Information Websites Identified through India's Major Search Engines. Advances in Preventive Medicine Volume 2016

Reidenberg, J R., Travis B, Lorrie F. C., & Brian F. (2015). Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding, 30 Berkeley Tech. L. J. 39 (2015)

Roca, J. C., García, J. J. & De La Vega, J. J., (2009). The importance of perceived trust, security and privacy in online trading systems. *Information Management & Computer Security*, *17*(2), 96-113.

Statista[1] (2016). Digital buyer penetration worldwide from 2014 to 2019. Accessed 24/5/2016 from Available at http://www.statista.com/statistics/261676/digital-buyer-penetration-worldwide/.

Statista[2] (2016). Retail e-commerce sales worldwide from 2014 to 2019. Accessed 24/5/2016 from http://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/

Tsai.J.Y, Egelman.S, Cranor.L, and Acquisti.A (2011) The effect of online privacy information on purchasing behavior: An experimental study. Info. Sys. Research, 22(2). retrieved from www.heinz.cmu.edu/~acquisiti/papers/...

Teufel H. III (2008) PRIVACY POLICY GUIDANCE MEMORANDUM. Memorandum Number: 2008-01 (2008). https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf

Turow, J., & Hennessy, M. (2007). Internet Privacy and Institutional Trust: Insights From a National Survey. New Media & Society, 9(2), 300-318. http://dx.doi.org/10.1177/1461444807072219

Udo Udoma & Belo-Osagie (2015). Data Privacy Protection in Nigeria: An overview of the Data Privacy Protection Laws in Nigeria. Available at http://www.elexica.com/en/legal-topics/data-protection-and-privacy/16-data-privacy-protection-in-nigeria

Uzun H. & Poturak, M. (2014). Factors Affecting Online Shopping Behavior of Consumers. European Journal of Social and Human Sciences, 2014, Vol. (3), № 3. Pp. 163-170

Wang, H., Lee, M. & Wang, C. (2008). Consumer privacy concerns about Internet marketing. *Communications of the ACM*. 41(3), 63-70.

Wurgler. F.M., (2015). Understanding Privacy Policies: Content, Self-Regulation, and Market Forces. 1-48. retrieved from www.law.uchicago.edu/files/file/mar