International Journal of Advanced Scientific Research | IJASR
International Journal of Scientific Research in Social Sciences & Management Studies | IJSRSSMS
ISSN Print: 2579–101X | ISSN Online: 2579–1928
Vol. 3, No. 1
April, 2018

Right to Privacy and its Effects on e-Commerce Adoption in Nigeria

[1]Taiwo Akeem A, [2]Bako Yusuf A. & [3]Olabimtan Rasheedat O.
[1,2&3]Department of Business Administration and Management,
Federal Polytechnic Ilaro, Ogun State

Abstract

E-commerce is basically a potent device for transformation of business which allows companies to improve their value-chain operation, extend to new markets, and enhance customers' service as well as providers. Internet security is a portion of information security framework and is applied particularly to the components that affects e-commerce which include computer security, privacy, data security and other fields of the information security framework. The objective of this research is to investigate the effects of privacy concern on e-commerce adoption by consumers in developing country with particular reference to Nigeria. The study inquired into level at which e-commerce has been adopted in the state sampled in Nigeria. Survey method was adopted to collect information from the respondents. The hypothesis was tested using regression analysis. The study revealed that security concerns and customers' information privacy among others are significant factors affecting the adoption of e-commerce by customers in Nigeria. However, it can be deduced from the findings that for e-commerce to grow in Nigeria, organizations, government and other stakeholders must provide proper legislation, good security and privacy systems as well as security data transmission and storage.

Keywords: *Right to privacy, Internet security, Diffusion, e-Commerce adoption, Developing economies*

Corresponding Author: **Oguchi, Chinweuba Benjamin**

Background to the Study

The explosion of internet technology into the global arena corresponds with the new millennium and the benefits of commercial uses of internet have since gotten out of control (Agwu and Murray, 2014). Internet technology has given access to new chance of advancement for businesses of all dimensions to conduct activities efficiently and effectively (Gharbi and Ashrafi, 2010). E-commerce is seen as the conduct of business amongst enterprises with the help of Information and Communication Technology (ICT), especially with the use of internet (Pita & Chris, 2011). Baseline (2006) defines e-commerce as the buying and selling of goods and services through electronic systems such as the internet and to a smaller extent, other computer networks. Generally, it is regarded as the sales and commercial function of e-business. The popularity of the internet has transformed the cultural commerce into e-commerce, which has shown to be a profitable operating system for various businesses (Rahman and Lackey, 2013). A large variety of commerce is carried out through e-commerce, which includes electronic funds transfer, supply chain management, internet banking, online transaction processing, electronic data interchange (EDI), inventory management systems and automated data collection systems (Ayo, Adebiyi, Fatudimu and Uyinomen, 2008). Sen, Ahmed and Islam (2015), noted that the implementation of the e-commerce application give advantages which would have been difficult without regular approach to e-commerce security and uninterrupted working on the security issues.

Traditional commerce which is done face to face with effort of an individual to go to organization and get the job done consumes time, but e-commerce has solve the problem (Niranjanamurthy and Chahar, 2013). Presently, e-commerce is facing challenges like security issues which is fundamentally part of information security framework and this security is particularly applied to the assets of e-commerce (Sen, Ahmed and Islam, 2015). The transmission of fraud data, data theft and sundry dangers to e-commerce such as harmful insiders, threats to communication, confidentiality threats, etc. hinders the adoption and development of e-commerce. Privacy is an old concept, but implementing it is still new in the field of e-commerce (Smith and Shao, 2007). It has turned into a major component of e-commerce strategy and the provision of better protection of consumers' privacy will lead to increase in consumer trust, spend and loyalty (Jebur, Gbeysari, and Roghanian 2012). Performing e-commerce activities requires a certain amount of information like personal bank account number or an address. A large number of people are unwilling to provide this information for fear of disclosing to others and exploit for illegal purposes (Meng, Yang, Xu, Zhang, Nie and Xian, 2009). Yazdanifard, Sadeghzadeh and Ojaroudi (2010), defined privacy as "the rights of individuals and organizations to determine for themselves when, how and to what extent information about them is to be transmitted to others". This depicts that one can only access the information if he or she is authorized.

Jebur et al. (2012), described privacy as an act of trade between two parties where exchange is negotiated on a set of conditions and satisfaction of both parties upon development of trust between the parties. They went further by saying that in order for organizations to gain the confidence of consumers, they must show the procedures for protecting consumers' privacy. Additionally, right security measures must be taken by the organizations in order to protect the

consumers' information during storage and communication to enhance their trust in the services provided to them (Yazdanifard et al. 2010). Based on the above, there is need therefore to explore the effects of customers' information privacy on the adoption of e-commerce by customers in Nigeria as a developing economy.

Statement of Problem

Nowadays, security and privacy are serious concerns for electronic technologies, and e-commerce shares security interests with other technologies in the field (Niranjanamurthy and Chahar, 2013). The concerns for privacy have been discovered to reveal lack of trust in various contexts, which include commerce, electronic health records, electronic recruitment technology and social networking, and this has a direct influence on users (Yazdanifard and Edres, 2011). Privacy has become a major interest for consumers with the increase in identity theft and impersonation, and any consumers' interest must be taken seriously by e-commerce providers (Raghallaigh, 2009; Niranjanamurthy and Chahar, 2013). Consumer right to privacy is becoming the most advertised issue of security that replaced theft and fraud as top concern in e-commerce which has restrain customers from using e-commerce (Randy and Joseph, 2002). Privacy is an old concept, but in the field of e-commerce, its implementation is still very new (Jebur et al., 2012). Privacy becomes a major component of e-commerce strategy and providing its better protection will lead to consumer trust, speed and loyalty. Al-Slamy (2008) in his study discovered that more than two out of every five people in North America are internet users and the web is becoming an integral part of daily life, and without an absolute privacy security policy, it will be impossible for customers to spend money in an accountable and economical manner. Privacy policies give the way in which an organization receives, uses, protects data and the choices they give to consumers to exert rights when their personal information is used (Ahmed & Hassan, 2016). With quick development of the internet and World Wide Web, computer and information system have more and more become the targets of criminal attacks and intrusions (Kaur, Patha, Kaur and Kaur, 2015). Protecting customers' information and data may be a serious concern for organization and this may debar customers from using e-commerce. The study therefore intends to investigate the effects of customers' right to privacy on the use of e-commerce among customers in a developing economy.

Objective of the Study

The objective of this study is to investigate the effects of customers' right to privacy on the adoption of e-commerce by customers.

Research Question

In what ways does customers' right to privacy affect the adoption of e-commerce?

Research Hypothesis

$\mathbf{H_{01:}}$ There is no significant relationship between customers' right to privacy and e-commerce adoption

Literature Review

Conceptual Framework

E-commerce

Electronic Commerce or e-commerce is seen as a wide range of online business activities for goods and services. It can also be referred to as any form of business activity in which the interaction between parties is electronically rather than physical exchange or direct physical contact (Chivasa and Hurasha, 2016). Turban, Lee, King, McKay, Lee and Viehland (2008) see e-commerce as the process which involves buying, selling, transferring or exchanging products, services and or information through computer networks, including the internet. E-commerce has been touted as an avenue to reach global customers by gaining market shares with lower cost (Agwu, 2012). This is however achieved by streamlining a large range of business processes and technology for competitive advantage using telecommunication and relationship improvement networks (Agwu and Murray, 2014).

Turban et al. (2008), distinguishes between internet and non-internet e-commerce. The non-internet e-commerce involves for instance to buy and pay services on goods with smart cards by using vending machines and/or transactions undertaking through network like Local Area Network (LAN), by the use of intranets or even single computerized machines. A few researchers view e-commerce in terms of applications of internets like intranet, extranet, website and email (Ayo, Adebiyi, Fatudimu and Uyinomen, 2008). Others see e-commerce as the alliance of business processes with internet technologies such as interactions with customers and suppliers (Iddris, 2012). Nevertheless, there is a common agreement among researchers that the key components of e-commerce include: website, email, intranet, extranet, LAN and Wireless Area Network (WAN), Voice Over Internet Protocol (VOIP) (Iddris, 2012). In Nigeria, the e-commerce industry started in the mid-nineties when the internet and telecommunications industry started going popular.

Its development was not fast until the arrival of internet banking at the commencement of the 21st century (Oluyinka et al. 2013). This is due to the fact that an e-commerce service is dependent on the ability of people to make use of the new innovation technology. Service such as electronic cash transfer has a large impact on the development of e-commerce in Nigeria (Bada, Okunoye, Omoyokun, Adekoya and Eyob, 2006). Businesses in Nigeria are facing gradual expansion, as e-commerce creates global advantages to open new markets that is lucrative for local goods and services at far and near distance (Oluyinka, et al., 2013). The systems of online shopping give consumers wider option as regards their desired goods and services, and present a lot in terms of ease and suitability as different from overseas travels for the purpose of shopping (Garbi and Arshrafi, 2010).

The researchers in Nigeria propose that for e-commerce adoption to be improved in Nigeria, the Central Bank of Nigeria (CBN) should consolidate a small number of banks on unprincipled potentially counterfeit on business practices and the scope (Oluyinka et al., 2013). By introducing this policy, CBN intends to reduce fraud and improve the confidence of the consumers on internet transactions (Park et al., 2007). Millions of young people can have access to the internet from the Wireless Application Protocol (WAP)—enabled mobile phones,

smartphones and their PCs using the hotspot on their phones. This is possible due to the introduction of General Packet Radio Service (GPRS) connectivity; the global system of mobile communication operators (Peersman, 2000). According to Kalakota and Whinstone, (1996), e-commerce is a cover concept to bring together a large range of available and new application.

Privacy Issues and e-Commerce Adoption

Privacy has now become an inherent component of any e-commerce strategy and placement of capital in protection of privacy has been seen to increase consumers' pay-out, trustworthiness and fidelity (Raghallaigh, 2009). Ackerman and Davis (2008) assert that privacy is an important issue in e-commerce, no matter what source it is examined from. Fisher (2001), reported that "forty-one percent of web buyers surveyed by Forrester Research of Cambridge said they have contacted a site to be taken off their database because they felt that the organization used their information unwisely." Also, Harry (2000) discovered in his research that forty percent of online buyers were very concerned about the use of their personal information, and 57% desired some kind of laws regulating how personal information is gathered and used. Likewise, Kraft and Kakar (2009) argued that privacy concerns were a crucial motive why people do not go online and when they go, they provide spurious information. Why is privacy a serious concern? The answer is straightforward. Hasan and Sobhan (2012) discovered that the most online businesses had failed to adopt even the most essential principles for equitable and pure information practice. In fact, relatively small number of consumers believe that they have extreme control over how businesses used and sold their personal information that was revealed online (Ackerman & Davis, 2008). The alliance of latest business practices, consumer anxieties, and the pressure of the media have made privacy a strong problem of e-commerce (Pita and Chris, 2011). Privacy has effects on e-commerce consumers and in addition, organizations or stakeholders (Jebur et al. 2012).

Annie and Julia (2000) propose self-regulation as means to address concerns about consumer privacy. In 1999, the Federal Trade Commission (FTC) issued a report to the United States Congress encouraging organization to address the concerns of consumers about privacy through regulation. Despite the fact that self-regulation had previously been supported and motivated, the report was still presented and most online business had still not adopted the basic practices that address consumers' privacy. From the consumers' point of view, many sites of e-commerce have done unwise things with the data of their customers (Ackerman and Davis 2008). Fisher (2001), observed that the opinions of consumers in this have been confirmed by media stories of a particularly conspicuous privacy failure and public relations displeasures. Speaking liberally, consumers are wholly confirmed in their judgment by the media. As reported earlier, a small number of customers trust businesses to keep their data private. Light (2001), in his survey, discovered that 92% of the respondents showed that companies would not keep the customers data private even if they promised to do so.

Jebur et al. (2012), argue that consumers have two types of privacy concerns. First is the concern over unauthorized access to personal information because of breach in security or the lack of internal control. The second is the consumer concern about the secondary use risk i.e.

the reuse of their personal information for the purposes that are not related to the original one without the consumers' consent. These unrelated purposes may include sharing the data with third parties who were never part of the transaction in which customer related his or her personal data. It as well includes the accumulation of consumers' transaction information and other personal data to produce a profile. Furthermore, Raghallaigh (2009); Niranjanamurthy and Chahar (2013), bring two other concerns based on Delphi studies, which are general concerns about personal data that are collected and concerns over one's incapability in correcting any errors. Further away from the research literature that describes a general apprehension (and its extent) there are some literature in the research that provides more details (Harris, 2000). A continuous finding for several years is that it is beneficial to consider US consumers comprising of three groups but not as a general block (Ackerman & Davis, 2008).

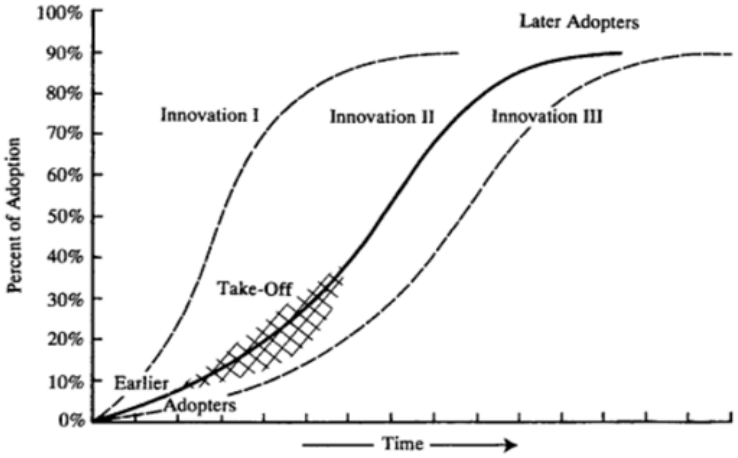
They include privacy fundamentalists, the pragmatic majority and the marginally concerned. The grouping have been consistent in various studies e.g. Ackerman & Davis (2008), Spiekerman, Jens & Bettina (2001). The pragmatic majority are divided by Spiekeman et al. (2001), into those who were considered with identity revelation and those who were more concerned about making available their personal profile. These 3 groups were 17%, 56% and 27% of the Samples respectively (Ackerman et al. 2008). Spiekerman et al. (2001), observed a greater group of privacy fundamentalist and a smaller marginally concerned in Germany. There are significant differences in the groups' preferences for privacy and attitudes. The marginally concerned group is mainly nonchalant in their privacy concerns. Conversely, privacy fundamentalists are quite inflexible about their privacy. However, large percentage of the US population is concerned about privacy but can trade personal data for some benefits (e.g. customer services).

Nevertheless, consumers in developing economies like Nigeria still want sufficient measures to guide and protect their data from unsuitable sale, accidental leakage or loss and intentional attacks. There is frequent significant reduction in the concerns of pragmatists by the presence of privacy protection measures like laws or policies on web sites (Ackerman et al. 2008). Organization functions such as e-commerce database management, security techniques, telecommunications, collaborative systems and systems implementation have impact on information privacy (Pennanen, Kappu and Paakki, 2006). In developing electronic commerce system, the developers need to be sensitive to the connection and recognize the need for advance privacy planning. Obviously, it is important to reflect on those factors all through the requirements determination and software design of e-commerce system.

Theoretical Framework

The Diffusion of Innovation (DOI) theory was chosen as a guiding theoretical framework for this study which is well known in the technological innovation literature and used to gain insight into the extent of e-commerce diffusion and adoption by consumers. DOI was developed by Rogers (1995) to describe how an innovation is communicated through certain passages overtime amidst social system members. Rogers (1995), identifies weighty characteristics of innovations as perceived by individuals. These are significant as they are represented in such a way that potential adopters may see the innovation.

Fig 1: Diffusion of Innovation



Source: Rogers, (1995)

The features that creates the base for what is regarded as perceived attributes of Innovation Diffusion according to Oluyinka, et al, (2013) includes:

1. Relative Advantage: This is portrayed as the extent to which the advantage of adopting e-commerce is perceived to be better than not adopting it. Relative advantage requests the buyers to appraise the benefits and detriments of using the e-commerce technology, which can be expressed in a social, economic and other ways.

2. Compatibility: This is the extent to which an innovation is perceived to be consistent with the value that has been in existence, previous experiences and needs for potential adopters. There is evaluation of social cultural values of potential e-commerce adopters in relation to the values and belief system, formal introduced ideas and needs of consumer for the technology.

3. Complexity: This is the extent to which an innovation is seen as difficult in understanding and use. Complexity considers the level of physical or mental endeavors required to use an e-commerce technology for daily business activities.

4. Trialability: This is the level to which an innovation can be put in experiment within limited base. It permits the adopter to have preliminary assessment of an innovation so as to give meaning to the adopter.

5. Observability: This is the level at which the outcomes of an innovation are viable to others. The earlier it is to see the outcome of technology by potential adopters, the more probable for them to adopt it. The more the innovation can be visible and be communicated by others, the greater the observability (Rogers, 1995).

Some of the characteristics of DOI are suitable for this study. It has been used in various past studies at the levels of individual and firm. Furthermore, its factors assist in understanding the

direction of the decision makers towards implementing the new mechanisms in workplace, specifically the information technology mechanisms like e-commerce (Oluyinka et al, 2013). For example, a large number of micro-enterprises in Nigeria operate in the informal sector of the country, and almost significant number of overseas-based firms were disconnected from the rest of the economy (Abdel-Nasser, 2012). Researchers on innovation diffusion are limited in developing countries and universal systems are not well connected to local realities, specifically to the needs and opportunities of labour market. This study take into account a brighter understanding of what is meant by innovation in developing countries as a crucial factor that progress e-commerce adoption. Factors such as internet security, trust, privacy, integrity, laws and regulations are influenced by innovation diffusion theory and consequently is crucial in determining adoption level of e-commerce in developing countries.

Empirical Framework

The adoption and use of ICT services such as e-commerce is greatly reliant on financial resources, network availability, bandwidth and the overall awareness by the general public (Chivasa and Hurasha, 2016). Nevertheless, Awagah, Kang, and Lim (2015), argues that e-commerce may result to relegation of developing nations particularly the SMEs. These tasks vary from ICTs infrastructure, narrow technological and knowledge diffusion. The security menace to e-commerce websites are persistently modifying as new menace are exposed daily (Hassan and Sobhan, 2012). According to security response, cybercrime was on the increase from 2006 per Symantec, greater than a million consumer logged per internet crime complaint center (IC 3), complaints about supposed and alleged online fraud or cybercrime and directed half a million grievances to law enforcement agencies.

Hassan and Sobhan (2012) explained that a survey by computer security institute in 2007 discovered 46% security breach; which resulted to 91% financial loss. Also, in 2008 survey, it was reported that the average annual loss increased from $168,000 in 2007 to $350, 424 in 2008 and underground economy marketplace that present sales of stolen information developing. According to Consumer Reports Money Adviser by Perrota (2008), the Attorney General of the US has announced multiple accusations that relates to an overwhelming breach in international security that involves nine major retailers and more than 40 million credit and debit card numbers. It was thought by US attorneys that it may be the greatest hacking and identity theft case ever tried by the justice department. It was mandated by both the EU and US legislation at the federal and state levels that organizations should inform customers about the use and disclosure of information.

Vail, Earp and Anitan (2008), explained that such disclosures are normally carried out through privacy policies both online and offline. In their study, Lauer and Deng (2008), presented a model that links privacy policy through trustworthiness, to online trust and then to customers' loyalty and their agreement to provide honest information. A sample of 269 responses was used to test the model. It was discovered that consumers trust in a company is closely linked with the perception of the company's respect for customer privacy. Similarly, trust is linked to increased customers loyalty that can be evident through increased purchases, trying new products, and the will to participate in programs that use extra personal information. A theoretical framework was developed by Head and Yuan (2001), for privacy protection in e-commerce to understand better the major parts and duties of diverse parties concerning privacy violation and protection. They established four main parties included in privacy protection:

1. The privacy subject i.e. the consumer,
2. The collector i.e. the company website,
3. The illegal user i.e. the violator, and
4. The privacy protector who protects the subject rights by preventing the violator and developing guidelines for the collector.

Head and Yaun (2001), discovered that it is very crucial for privacy to be protected in marketplace by ascertaining the activities and the movement of information amidst various privacy parties. Jebur et al. (2012) established that privacy and security are notable issues for both e-commerce and consumers. The latter is concerned about their financial data while the former is concerned with the financial losses resulting from the infiltration and revealing the confidentialities of customers and the company. They laid more emphasis on organizational policies that support security and privacy achievement. Protection of consumers' privacy is important and useful to e-commerce and consumers alike (Smith and Shao, 2007). The protection of consumer privacy is not an easy task because the privacy includes security problems of the stored and transmitted data. These difficulties are technical and non-technical like laws and regulation, strategy measures, commercial idea and others (Meng, et al, 2009). It is important to develop new standards in order to secure consumers' privacy for e-commerce to grow and to enact sufficient laws to guarantee consumer privacy. There should be cooperation among consumers, companies and government to ensure the protection of consumers' privacy rights (Kraft and Kakar, 2009). We can see that privacy is a major concern to users and in the event of compromising their privacy, customers become very disturbed and there is a general negative effect on trust in e-commerce (Vail et al., 2008).

Clemes, Gan and Du (2012), asserted that due to the warnings that are increased by the media from security and private breaches such as identity theft and financial fraud, and the promoted consciousness of online customers about the threats of performing transactions online, e-commerce has not been able to accomplish its whole potential. Niranjanamurthy and Chahar (2013), discovered that many customers refuse to perform online businesses and that is related to the lack of trust or fear for the leakage of their personal information. The traditional authentication mechanism is based on identity to provide security or assess control methods; additionally, traditional encryption and authentication algorithm demands high computing power of computer equipment. E-commerce gives the organizations chances, but also causes a set of new risks and vulnerability like security threats. Therefore, securing information is an important management and technical requirement for any effective and efficient payment transaction activities through the internet (Farshchi, 2011). Baseline (2006) stressed that security fears about e-commerce have resulted in loss by retailers to an estimated $2bilion in 2006 as reported by Gartner survey of 5000 U.S adults. Also, roughly one-half of those casualties ($913 million) could be predicated on people who shunned sites that appeared to be less secured and the remaining about ($1 billion) came from consumers who were so much afraid to transact e-commerce business at all. It was also reported by Pressman and Lowe (2009) that some 33 million U.S adults avoided online banking due to security concerns.

Another report by Forrester Research gave an estimate of $15 billion electronic retailers' loss in 2001 because of privacy of consumers. Consumers do not trust sites of e-commerce to be secured and respectful of their privacy (Smith & Shao, 2007). In spite of these concerns, e-commerce plays a very significant role in the development of industry as an effective, expedient and quicker methods of transacting business (Kraft and Kakar, 2009). As online transactions

trend keeps on growing, there will be increment in the quantity and categories of attacks against the security of online payment systems. Such attacks threaten the security of the systems, which results to systems that may be compromised and less protected, resulting in consumer privacy issues (Baseline, 2006). Consumers may be at the risk of losing their personal data, since they may be unaware of the security aspect of performing online transactions (Kraft and Kakar, 2009).

Methodology

The aim of this study is to unravel the effects of customers' information privacy on the adoption of e-commerce by customers in Nigeria as a developing country. This study requires the input of individuals from different parts of Nigeria, different ethnicity, race, education, income levels and beliefs, hence, survey method was adopted. Survey method was adopted because it was an inexpensive and efficient means of gathering information from the targeted population (Oluyinka et al, 2013). The survey environments were three zonal headquarters in Nigeria which are Ibadan, Enugu and Kaduna. Ibadan was chosen because it was zonal headquarter of the Western Nigeria, Enugu was chosen to represent the east and it is also the political capital, while Kaduna was selected to represent the Northern part of Nigeria. However, the instrument for data collection was pre-tested in two polytechnics in Ogun-state—Federal Polytechnic Ilaro and Moshood Abiola Polytechnic, Abeokuta with different ethnic group in attendance. Using a convenience sampling technique, the survey questionnaire was administered to 240 respondents at 80 per city using simple random sampling technique. The administration and collection of the responses lasted 4 weeks. Two hundred and twelve (212) copies of questionnaire were collected back. It was discovered in the course of the analysis that twelve questionnaires were not filled completely, hence cannot be used and were voided. At last, two hundred questionnaires were deemed fit, which gives 84% response rate and were regarded suitable to be used in the study.

Data Analysis

Demographic profile of Respondents

This study respondents (table 1) are from various regions of the community and in addition various educational, social, cultural and ethnic backgrounds. The results of demographic profile shows that 72% were males and 28% were females. The largest group in this study comprised of those aged 31-50 years which portrays 62.5% of the sampled population. These groups could be regarded as those within their agile working career and hence, very essential for this study and as a matter of fact, a very significant part which organizations cannot turn a blind eye. The addition of full time employees and self-employees which consists of 61.5% of the sampled population also gave the study the data that is very rich. These sectors of the population sampled are the possible users of e-commerce services.

Table 1: Demographic profile of respondents

Gender	Male	144	72%
	Female	56	28%
Age	20-30	42	21%
	31-40	68	34%
	41-50	57	28.5%
	51-above	33	16.5%
Marital Status	Single	61	30.5%
	Married	132	66%
	Divorced	4	2%
	Separated	2	1.5%
Qualification	WAEC/SSCE	46	23%
	ND/NCE	82	41%
	HND/BSC	42	21%
	MASTERS	19	9.5%
	OTHERS	11	5.5%
Employment Status	Full time	51	25.5%
	Part time	36	18%
	Not in employment	41	20.5%
	Self-employment	72	36%
Work Experience	5-10 years	74	37%
	11-15 years	52	26%
	16-20 years	54	27%
	21-25 years	19	9.5%
	26 years-above	1	0.5%
Income Level	10,000-50,000	16	8%
	51,000-100,000	23	11.5%
	101,000-150,000	26	13%
	151,000-200,000	34	17%
	200,000- above	101	50.5%

Source: Field survey, 2017

Test of Hypothesis

H_1: There is no significant relationship between customers' right to privacy and e-commerce adoption.

Table 2 shows R test result of 0.133 in the model, adjusted R-square test result of 0.015 which indicates that there is a very weak relationship between e-commerce adoption and joint effect of privacy variables used for the independent variable. The R-square test shows only 1.8% variation in e-commerce adoption that can be explained for by variables used for privacy. This also shows that there are other variables that determine e-commerce adoption that were not considered in the course of this study.

Regression

Table 2: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.133	.018	.015	.869

Table 3: ANOVA[a]

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	5.320	5	1.064	1.408	.020
	Residual	297.680	394	.756		
	Total	303.000	399			

a. Dependent Variable: I will adopt e-commerce for my transactions

However, in table 3, the ANOVA result indicates the significance of the hypothesis tested and shows that there is a significant relationship between customers' right to privacy and e-commerce adoption. It also signifies that the model used is adequate in relating e-commerce adoption and customers' right to privacy. Therefore, the Null hypothesis is hereby rejected.

Table 4: Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	4.653	.369		12.594	.000
	Access To Transaction Information	.146	.065	-.125	-2.232	.020
	Customers' Control of Information	.076	.049	.084	1.550	.012

a. Dependent Variable: E-Commerce Transaction(ECT)

$$ECT = 4.653 + 0.146\,ATI + 0.076\,CCI$$

The model shows that customers having full knowledge of the parties that can access transaction information will adopt e-commerce. Access to transaction information is significant with p-value of 0.020 and it affects e-commerce transaction positively. Also, customers' control of information will enhance e-commerce adoption positively and it is significant with p-value of 0.020.

Discussion

The objectives of this study is to investigate whether a significant relationship exist between independent variable (customers' right to privacy) and the dependent variable (e-commerce adoption). It was shown in the results that customers' right to privacy related positively to the adoption of e-commerce by customers. The findings have contributed in terms of establishing an understanding of some of the factors that influence the adoption of e-commerce by customers in Nigeria. Since the outcome of this study is in accordance with previous research results, it can be generalized not only to other states in Nigeria but other countries as well. For example a similar study by Yousafzai et al. (2007) to 441 internet banking users in Halifax Bank in Cardiff, United Kingdom found that perceived security and privacy are key components in the customers' acceptance, adoption and use of internet and e-commerce, thus they are worthy of particular attention. However, another study conducted by Shaharudin et al. (2012) discovered that perceived security and privacy were insignificant on e-commerce adoption among consumers in Malaysia. This is because majority of the respondents were not ICT compliant and therefore do not ascribe any benefits to e-commerce adoption. The result of this

study is also complemented by Agwu (2013) who carried out similar research to 630 customers in three big cities of the United Kingdom namely- London, Birmingham and Manchester. It was discovered that the elders and most business owners sees perceived risks in terms of security and information privacy as barriers to the adoption of e-commerce. Nevertheless, the youths care less about the perceived security and privacy. Moreso, a study by Kraft & Kakar (2009) in USA revealed that security concerns and consumers' privacy are the major factors that affects the adoption of e-commerce by customers. On the other hand, it was revealed in a study by Clemes et al. (2012) that perceived security and privacy concerns were insignificant to the adoption of e-commerce by customers, he however discovered some other factors or variables which includes convenience, user friendly website, internet access, perceived price, self-image, customers age, marital status, level of education, income levels among others that are significantly related to the e-commerce adoption by customers. Without de-emphasizing the impact of traditional methods, the adoption of e-commerce is capable of bringing so many benefits to customers. Based on the data, it is obvious that significant effects of perceived security and privacy concerns validates the fact that e-commerce can only be adopted when customers are assured of the security of their internet transactions and protection of their personal data and information.

Limitations and Future Research

In studying consumer behaviour, there is always the issue of generalization, and this particular study is not exempted. The sample size in Lagos, Abuja and Port-Harcourt, profiles of the respondents and the time of study may have affected the result. Future research can be expanded to other states, setting and times. Also, the sample size of 240 with population of more than 15 million may also have affected the results. Furthermore, the use of three cities in Nigeria where the level of education and availability of internet services are very high, which cannot be compared to others in the North West or North-East Nigeria may have also affected the study outcome. Future research could be carried out in other states in Nigeria. Whether the result of this study can be generalized to non-users or inactive users of internet and e-commerce will demand further research.

Conclusion

The benefits of e-commerce widely exceed the undesirables. There is possibilities of a very big success for businesses that practice e-commerce if potent security technologies are aided. The sales in e-commerce are increasing but privacy issues are coming into light as many consumers are concerned about the protection of their personal information. There is need to address privacy issue as it is important to the growth of e-commerce. Survey by Kraft et al. (2009) shows that e-commerce is losing a significant amount of income due to privacy and security concerns of its potential user base. Online organizations must have the "ability to give consumers control of their privacy in an attempt to create an acceptable level of trust which is essential" (Kraft et al., 2009). There are various security techniques that can be instigated by any e-commerce provider to reduce significantly the risk of attack and compromise. Risk awareness and the implementation of the multi-layered security protocols, detailed and open privacy with strong measures of authentication and encryption will go a long way to give assurance to consumer and ensure the minimization of the risk of compromise. The findings of this research shows that there exist a significant relationship between customers' right to privacy and their adoption of e-commerce in developing economies. The research contributes to the existing body of knowledge that there is need to guarantee consumers' right to privacy of the information provided and their consent be sought before their personal information are used for any transaction. This will enable them to embrace and adopt e-commerce in their various transactions.

Recommendation

It is very important that organizations should recognize that while it is extremely obvious that customer's relationship with the organization is to have a beneficial use and efficient e-commerce transaction, the perceived security and information privacy are also essential aspects of the association and add to the value. Organizations should build user friendly websites but must also include security building mechanisms that can protect malicious attacks on users without their knowledge or consent. It is imperative for e-commerce businesses to have the capability to give customers of their privacy in an effort to produce an acceptable level of trust. In addition, to reduce customers' security concerns, managers should adopt privacy policies to safeguard the customers' data against attack. Furthermore, a proper security and privacy legislation, self-regulation, technical solutions and vigorous solution adopted by organizations may reduce privacy concerns.

References

Abdel-Nasser, H. Z. (2012). Barriers to e-commerce in Egyptian SMEs. *International Journal for Information Engineering and Electronic Business, 3* (2), 9-18.

Ackerman, M. S., & Davis, D. T. (2008). Privacy and security issues in e-commerce. *Journal of Emerging Trends in Computing and Information Sciences, 5* (4), 28-36.

Agwu, M. E. (2015). Analysis of obstacles to uptake of internet banking services in Nigeria. *Research Journal of Business Management, 2* (1), 99-114.

Agwu, M. E., & Murray, J. P. (2014). Drivers and inhibitors to E-commerce adoption among SMEs in Nigeria. *Journal of Emerging trends in Computing and Information Sciences, 5* (3), 192-198.

Agwu, M. E. (2012). Generations X and Y's adoption of internet and internet banking in Nigeria: a qualitative study. *International Journal of Online Marketing, 2* (4), 68-81.

Ahmed, J, U., & Hassan, H. (2016). Barriers to E-Commerce Adoption in Syria: An Empirical Detection. *World Journal of Business and Management, 2* (1), 41-55.

Al-Slamy, N. M. A. (2008). E-commerce Security. *International Journal of Computer Science and Network Security, 8* (5), 340-344.

Annie, I. A., & Julia, B. E. (2000). Strategies for developing policies and requirements for secure electronic commerce systems. *Journal of Internet Banking and Commerce, 13* (2), 28-37.

Awagah, R., Kang, J., & Lim, J. I. (2015). Factors affecting E-commerce adoption among SMEs in Ghana. *Information Development Journal*, *2* (1), 1-22.

Ayo, C. K., Adebiyi, A., Fatudimu, I. T., & Uyinomen O. E. (2008). A framework for e-commerce implementation: Nigeria a case study. *Journal of Internet Banking and Commerce, 13* (2), 58-67.

Bada, A. O., Okunoye, A., Omojokun, A., Adekoya, A., & Eyob, E. (2006). Globalization and the Nigerian banking industry: efficiency and legitimacy considerations in the adoption of electronic banking (e-banking) services. *International Journal of Management and Decision Making, 23* (3), 23-26.

Baseline, G. (2006). *$2 Billion in E-commerce sales lost because of security fears*. New York, NY: Ziff Davis Media Inc,

Chivasa, S., & Hurasha, C. (2016). Small and medium enterprises (SMEs) adoption and usage of e-commerce: A Probit Modelling. *International Journal of Economics, Commerce and Management, 4* (3), 218-226.

Clemes, M. D., Gan, C., & Du, J. (2012). The factors impacting customers' decisions to adopt internet banking. *Bank and Bank Systems, 7* (3), 33-50.

Farshchi, S. M. R. (2011). Study of security issues on traditional and new generation of E-commerce model. *International Conference on Software and Computer Applications-IPCSIT, 9* (1), 24-31.

Fisher, S. (2001). Privacy by design. *Info World, 23* (27), 20-22.

Gharbi, K., & Ashrafi, R. (2010). Factors contributing to slow internet adoption in Omani Private Sector Organization. *International Journal of Computer Science and Network Security, 8* (5), 200-220.

Harris, P. (2000). *Online privacy: A growing threat*. Business Week. March, 20-96.

Hasan, R., & Sobhan, M. A. (2012). Study on e-commerce threats and security. *National Conference on Communication and Information Security.* Daffodil International University, Dhaka, Bangladesh. 76-83.

Head, M., & Yuan, Y. (2001). Privacy protection in electronic commerce: A theoretical framework. *Human Systems Management, 20* (2), 149-160.

Iddris, F. (2012). Adoption of e-commerce solutions in small and medium-sized enterprises in Ghana. *European Journal of Business and Management, 4* (10), 48-57.

Jebur, H., Gheysari, H., & Roghanian, P. (2012). E-commerce reality and controversial issue. *International Journal of Fundamental Psychology & Social Sciences, 2* (4), 74-79.

Kalakota, R., & Whinston, A. B. (1996). *Frontiers of electronic commerce.* Readings: Addison-Wesley.

Kaur, K., Pathak, A., Kaur, P., & Kaur, K. (2015). E-commerce privacy and security system. *Kuldeep Kaur International Journal of Engineering Research and Applications, 5* (6), 63-73.

Kraft, T. A., & Kakar, R. (2009). *E-commerce Security*. EDSIG. Washington DC. 1-11.

Lauer, T., & Deng, X. (2007). Building online trust through privacy practices. *International Journal of Information Security, 6*(1), 323-331.

Light, D. A. (2001). Sure, You Can Trust Us. *MIT Sloan Management Review, 43*(1), 17.

Marchany, R. C., & Tront, G. (2002). E-commerce Security Issues. *Proceedings of the 35th Hawaii International Conference on System Sciences. 2002 IEEE.*

Meng, X., Yang, J., Xu, X., Zhang, L., Nie, Q., & Xian, M. (2009). Biodiesel Production from Oleaginous Micro-organisms. *Renewable Energy, 34*(1), 1-5.

Niranjanamurthy, M., & Chahar, D. (2013). The study of E-commerce security issues and solutions. *International Journal of Advanced Research in Computer and Communication Engineering, 2*(7), 1-12.

Oluyinka, S., Shamsuddin, A., Wahab, E., Ajagbe, M. A., & Enegbuna, W. I. (2013). A study of electronic commerce adoption factors in Nigeria. *International Journal of Information Systems and Change Management, 6*(4), 293-315.

Peersman, C. (2000). The global system for mobile communications short message service: personal communications. *Institute of Electrical and Electronics Engineers*, *7*(3), 15-23.

Pennanen, K., Kaapu, T., & Paaki, M. K. (2006). Trust, risk, privacy and security in e-commerce. *Paper Presented at the Proceedings of the ICEB+ eBRF Conference.*

Perrotta, N. (2008). Be on guard for ID-theft schemes. *Consumer Reports Money Adviser, 5*(1), 2-22.

Pita, J., & Chris, J. M. (2011). E-commerce and the media-influences on security risk perceptions. *Information Security Group Royal Holloway, University of London. Egham, Surrey TW20 OEX, UK.*

Pressman, R., & Lowe, R. (2009). *Web engineering. A practitioner's approach*. McGraw Hill Higher Education, New York, N.Y.

Raghallaigh, E. (2009). *Major security issues in e-commerce.* Free Press, New York, NY.

Rahman, M. A., & Lackey, R. (2013). E-commerce systems security for small businesses. *International Journal of Network Security and its Applications, 5*(2), 193-210.

Rogers, E. M. (1995). *Diffusion of innovation*. Free press, New York, NY.

Sen, P., Ahmed, R. A., & Islam, R. (2015). A study on e-commerce security issues and solutions. *International Journal of Computer and Communication System Engineering, 2*(3), 425-430.

Shaharudin, M. R., Omar, M. W., Elias, S. J., Ismail, M., Ali, S. M., & Fadzil, M. I. (2012). Determinants of electronic commerce adoption in Malaysian SMEs' furniture industry. *African Journal of Business Management, 6*(10), 3648-3661.

Smith, R. & Shao, J. (2007). Privacy and e-commerce: A consumer-centric perspective. *Electronic Commerce Journal, 7*(1), 89-116.

Spiekerman, S., Jens, G., & Bettina, B. (2001). E-privacy in 2nd generation e-commerce: privacy preferences versus actual behavior. *Proceedings of the ACM Conference on Electronic Commerce,* 38-46.

Turban, E., King, D., McKay, J., Lee, J., & Viehland, D. (2008). *Electronic commerce: A managerial perspective*. New York: Prentice Hall, NY.

Vail. M. W., Earp, J. B., & Antan, A. L. (2008). An empirical study of consumer perceptions and comprehension of web site privacy policies. *IEEE Transactions on Engineering Management. 55,* 442-454.

Yazdanifard, S., Sadeghzadeh, R. A., & Ojaroudi, M. (2010). Ultra-wideband small square Monopole Antenna with variable frequency band-notch function. *Progress in Electromagnetics Research C, 15,* 133-144.

Yousafzai, S., Pallister, J., & Foxall, G. (2009). Multi-dimensional role of trust in internet banking adoption. *The Service Industry Journal, 29* (5), 591-605.