Actual and Perceived Consequences to Improper Online Privacy Management: A Pragmatic Approach

Zainab B. Nurudeen, Rashad Yazdanifard, and Abdullahi A. Nasiru

***Abstract*—With the world now becoming a global village, most business have over the years migrated their businesses online commonly known as e-commerce. Though this new technology brings about a wider market reach and faster marketing for most companies, it has also raised the issue of trust between business owners and their customers. The customers want to be sure that their information will be kept private and also be conducted in a timely fashion accurately. The intention of this paper is to discuss the main issues concerned with consumer online privacy, how best to tackle these issues, possible technologies to address these issues and also focus on an aspect that has not been researched as much i.e. The user's online privacy perception.**

***Index Terms* —E-Commerce, consumer online privacy, trust, privacy perception.**

I. Introduction

The main problem for users in the online world is the chance of being identity being stolen, but it is impossible for them not to leave some traces of their identity when using an online portal to make purchases or any other transactions. [1]. most previous researcher have only focused on the privacy issues that users face but there are other kinds of privacy aspects that should not be overlooked. they are:

a. Social Privacy: a person's right to not be exposed to unsolicited communication and the right to be secured and private.
b. Physical Privacy: a person's right to not being supervised in their personal area.
c. Psychological Privacy: a person's right to freedom of speech without any pressure to do otherwise.

Following the rapid evolution of networks from the limited ARPANET to the multi-billion user internet, the world is now considered a global village and like villages go, trading, exchanges and other forms of human dialogue are indispensable. Reliance on the internet is now prevalent vis-a-vis mobile communication devices as well as social networking applications that interoperate on globally computerized platforms [1]. The internet is not owned by anybody neither is it controlled by any organization, Thus in spite of the best efforts of regulatory authorities such as the Internet Engineering Task Force (IETF),International Telecommunications union (ITU).,who develop protocols and guidelines for Internet use, the internet is indeed an open ground where various activities, nefarious and otherwise are abound.

Following the above, there is the need to ensure the privacy of participants engaged in trade/contract over the internet. Privacy is the right of an entity to self determination with respect to the degree to which their personal details are revealed [2]. Online privacy, loosely translated as internet privacy can be said to be the individual/organization's desire of personal privacy in matters concerning it over the internet. This desire can be further extended to exercise the individual/organizations right to determine exactly who can access their information and to what extent over the internet. The onus of providing this function rests with the service provider be it a bank, supermarket, government organization or an e-mail service provider. This is not to say consumers do not have a responsibility to keep their online particulars private as well as ensure compliance with online privacy policies of organizations. E-commerce sites, online banking applications, information warehouses and social networks are all but a few of avenues in which online privacy is required and are susceptible to compromise. There are various ways by which cyber thieves steal consumer identities online, Phishing being the most popular and successful one.

Phishing is one of the many ways in which attackers retrieve information online through the creation of bogus websites by requesting for particulars such as usernames & passwords from consumers [3]. There have been several celebrated cases of online privacy breaches which have resulted in identity theft thus leading to data loss, online fraud, trust exploitation and a myriad of other unsavory attacks. A recent example in the Times Series Newspaper is that of David Peters, a man caught with 128 identities in the UK in July 2011.He used these identities to perpetrate frauds of up to £636,000. Most Online users are prone to online identity theft the moment they have caused to transact any business online. Most websites have an online privacy notice which most consumers have failed to read. These notices are intended to promote consumer choice and reduce the risks of disclosing personal information online. But putting up these notices would have no effect if unread by consumers. There

Manuscript received October 9, 2011; revised February 10, 2012.

Z. B. Nurudeen is with Multimedia Management in Limkokwing University of Technology, Cyberjaya, Malaysia. (E-mail: zainab.nurudeen@gmail.com).

R. Yazdanifard is with Limkokwing University of Creative Technology in Center Of Post Graduate Studies and Faculty of Information and Communication Technology located in Cyberjaya, Malaysia. UCI (Unity College International) was his previous Employer (e-mail: rashadyazdanifard@yahoo.com).

A. A. Nasiru is currently undergoing Msc. In Computer Networking in Limkokwing University of Technology, Cyberjaya, Malaysia. And is on study leave from the Lagos state University, Lagos, Nigeria (e-mail: nasbanjo@hotmail.com).

are various online behaviors that may increase or reduce risk of online identity theft. This article will attempt to discuss the ways online identity theft occurs and help users understand how their actions online make them susceptible to these thefts and giving undue advantage to third parties to have access to their personal information.

II. Possible Threats to Consumer Online Privacy

Organizational efficiency is constantly endangered by multidimensional security threat [4]. Compromise of consumer online privacy can be broadly classified as passive attacks and active attacks. Invariably the successful execution of the passive form of attack gives leeway to engage in an active attack.

Passive attacks seek information from a network system without altering the information either in transit or in-situ. Knowledge gained from the information gleaned can be used for purposes such as competitive pricing, technology stealing and other unfair leverages.

This form of attack is very difficult to detect as no information is altered and all seems normal [5]. A passive attack is defined as characterized by the observation/analysis of transmitted messages [5]. The International Telecommunication Union, ITU in consider passive attacks as exemplified in traffic flow analysis, release of message content, observation of data etc. [6].

Various tools and utilities are used to carry out this form of attack. Among them are phishing, phreaking, skimming and pretexting.

Given that information security requirements of any organization must satisfy the cardinal demands of

- Confidentiality
- Data Integrity
- Data Authentication
- Access-control
- Non-repudiation
- Availability

III. Effects of Consumer Online Privacy Compromise

The rate at which customers participate in online surveys & related activities is highly hindered due to concerns relating to the privacy of their personal information[7], [8]. Effects of online privacy compromise could be felt socially, economically and politically.

The social effects include loss of trust and invasion of privacy, the economic effects include identity thefts and use of information while the political effects relate to Government use of citizens data.

Emergence of highly digitalized technological advancements have paved the way for government to introduce channels through which it could pass along information to its citizenry as well as exchange information with sister government agencies.

The deluge of information is at its disposal which could include basic required information as well as secondary information thereby generating controversy amongst those concerned. This information is often regarded as private. Amongst the controversy generated are demands on the government to respect privacy concerns of the citizenry, the confidence of the citizenry in the government to securely keep their information, and the means by which (electronic or otherwise), communication with government takes place [9].

Identity Theft**:** Identity theft is a situation whereby data about an entity is obtained fraudulently in order to take advantage of a commercial relationship the entity has had with a service provider thereby empowering the thief to carry out transactions such as making purchases while the entity (owner of the information) bears responsibility [10]. In the study carried out by Unisys (2009), in order of priority, identity theft followed by financial fraud was discovered to be of utmost concern for consumers. In fact, with reference to the banking industry, 75% of respondents would react to loss of trust issues by switching to other banks where better protection for privacy is guaranteed [10]. Recent cases of data breach are that of Sony Play station Network where it was alleged that details of about 77 Million members of Sony Play station Network are in jeopardy. Identities if not used directly by the thief to perpetuate harm are often placed on the black market for others to purchase. Research over the years has given an insight to the financial insight of stolen identities in the black market. A stolen identity costing $100 3 years ago, now go for as low as $14 [11]. Andreas M. Antonopoulos attributes the sharp decline of price of stolen identity to an increased efficiency of the black market operations resulting in huge numbers of stolen identity thus the reduction in price. Online Fraud is an offshoot of Identity theft**;** annually, internet fraud is a cause for losses in consumer funds. There is a 57.43% increase in fraud related consumer losses between 2004 & 2005 [12].There are various types of scams that online consumers are susceptible to, one of them is the general merchandise fraud which is characterized by hijacking consumer purchases online so that merchandise purchased are not delivered to the buyer. Another type is credit card fraud which is perpetrated by theft of credit card details of an entity and making transactions in the card holder's name. An example of where this has been carried out is on the popular payment platform, PayPal. A spoof of the platform website was created & fed via email to customers requesting for detailed information such as social security numbers, date of birth, driver's license number, credit card numbers etc. [13]. Breach of consumer online privacy paves the way for online fraud to be perpetrated.

- Use of Information: Failure of information security measures is a cause of a number of security incidents. This failure could be due to technical reasons, managerial reasons, organizational reasons or human reasons. An example of organizations that have experienced inadequate security measures are choice point & time Warner. However, there are organizations such as Double-click & Amazon who considered it legitimate to make use of consumer information in their custody [14]. Failure to protect consumer information could lead to its exposure to unauthorized people; they could use this information to gain a marketing edge, technological advantage and other forms of unfair leverages. Also in the mix are third party sites that are present on sites used by parties. These third party sites gather information sometimes for marketing purposes without necessary due

permission from the consumer. There are tools that enable users know if there are third parties present on websites they are surfing. These tools however, do not let users know what the third parties do with the information they gather [15].

- Invasion of Privacy: The knowledge that his/her online information is susceptible to being viewed by a third party can create a psychological fear in the consumer. The fact that there are no recognized/standardized definitions of privacy hence weak laws protecting it further buttresses the consumers' fears. Inexactitude in the concept of privacy is a bottleneck. Hence it means different things to different people. By virtue of this the term "protecting privacy" is an unclear concept [16]. It is said that lack of clearly defined legal policies to prosecute invasion of privacy is one of the many factors that has contributed to growing sensitivity to information privacy [16] [16], contributing to this invasion are consumer group lobbying activities such as those of electronic privacy information center [17]. The overall effect is the loss of trust of the consumer in the service provider system. The service provider could be an e-commerce site, a bank, payment gateways, gaming platforms and any other form of interface the consumer relates with. While there are many reasons that contribute to shoppers avoiding making purchases on websites, studies have shown that a fundamental reason is lack of trust [18]. Corporate credibility which is composed of personal trustworthiness & expertise can be said to be the extent to which a company can deliver goods and services in meeting up with the consumer's expectation [19] [20].

There are several factors that could affect an individual's privacy fears [21]. These factors are depicted in the diagram below.

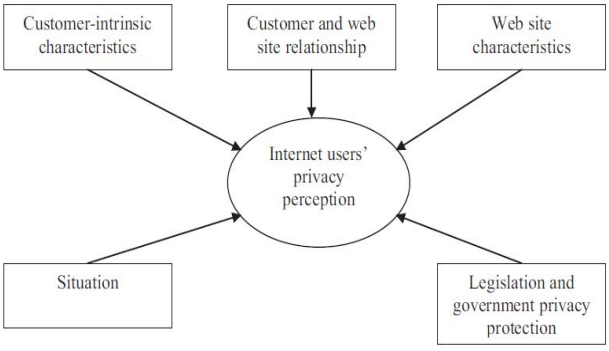

Fig. 1. Online Privacy factors influencing privacy perception of online users [21].

a. Customer-Intrinsic Characteristics: These are factors that contain individual centric information about users such as demographic data, privacy victim, internet experience, and privacy segmentation. All these affect their privacy perception [21]. The term privacy victim refers to a person who has had his personal information in an unauthorized manner such as receiving unsolicited mails and defamation by a third party. Privacy Segmentation is a mechanism by which users are divided into groups according to how they are sensitive to their privacy: 1) users unconcerned about their privacy, 2) Privacy Fanatics, 3) Privacy sleuths [21].

b. Customer and Website Relationship: this is determined by the customer's "general attitude towards the way their information is being requested and collected by the website. This has to do with how much access the customer has to the information he has furnished to the website, whether he is allowed to view, edit or even delete information at will. Although a customer has given his information to an organization, he would still like to have some control over it and also be able to trust the organization from keeping the information from unauthorized persons both within and outside the organization [21].

c. Web Site related factors: this has to do with how the user perceives the web site in term of how familiar the user is with the company brand, perceived integrity, perceived risk, web service quality, perceived credibility, perceived benevolence and company reputation. If a user is accustomed to a particular brand especially if it is a popular brand. Generally, customers do not like web sites that ask for their personal information but may be incline to re-think if it's a brand they know about. The integrity of a website is how the user perceives the level of trust he has for the organization and also how he perceives the honesty and sense of obligation of the organization. If the user has a good perception of the organization's integrity, this would reduce his privacy concern. Perceived Risk in its entirety is how a customer perceives the company's behavior in safeguarding his information and not exposing or selling it to a third party. Web Service quality is how a customer reacts and appreciates the level of service provided by the organization [21].

d. Situational factors: Users react in differing manners when doing the same transaction as they might have done earlier. This could be due to the relevancy of the information being requested by the website. Therefore situational factors should not be neglected [21].

e. Legislation and government privacy protection: This is related to matters involving the law and government in protecting user's privacy when online. These factors are important to users because they feel safer knowing that there are laws protecting an organization right to use their information and also that the government has put up some laws in place to also protect their information. So it is good for customers to know that the websites they are using have to follow some certain guidelines as regards their data [22].

The diagram below is referred to as the User's Privacy Perception. It was used as a research model for e-banking/online shoppers [22].

The Results of the survey showed that the users had a relatively high level of satisfaction from the privacy protection on a general level but this did not correlate with their privacy perception. This could mean that during the actual transaction they did not notice anything that was bothersome but somehow they still do not feel totally protected [22].

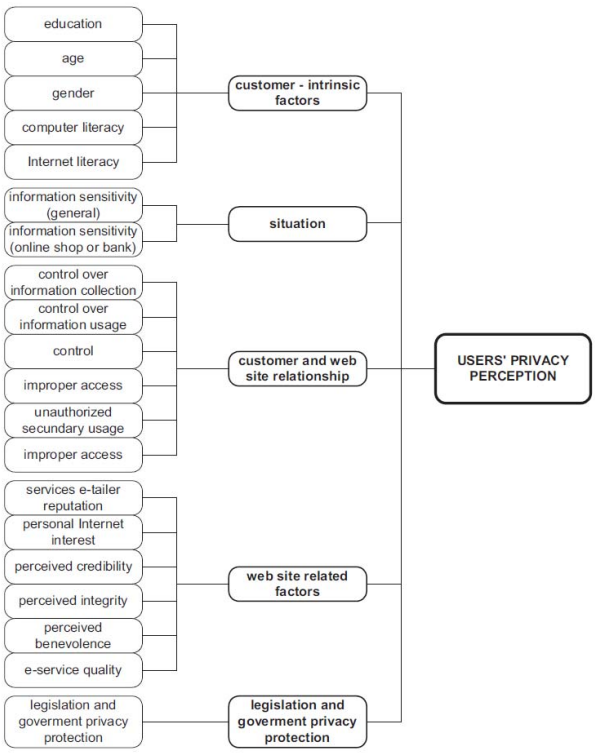

Fig. 2. Research model of e-banking/online shopping users' perception [22].

IV. Online Privacy Issues in the Mobile World

Privacy is defined as an individual's right to not being exposed to unsolicited publicity, the right to live without disturbance by the public especially in matters not concerning them, simply the right to be left alone[23].

In the mobile World, users share some data with the service provider; this could either be insignificant data or data containing personal information about the user. In turn the service provider could provide a customized or a basic service thus introducing the concept of service personalization which is dependent on two factors: [23]

a. Consumer's will to share their personal information and use provided personalized services.
b. Service Provider's capability and obtaining and handling the consumer's information.

A study from Nokia Siemens Networks identified three major types of users:

a. Selective users: these are practical users who are willing to give out some personal information in return for personalized services.
b. Afraid users: these type of users are very protective of their data and only disclose little amounts of information
c. Uninvolved users: these are mostly young people who are ignorant of privacy infringement issues.

The framework below assesses business models for privacy management [23]

This model can be viewed as similar to the Prisoner's Dilemma model used in economics where each person gives out some piece of information hoping the other person would do the same. This way, each person can provide as much information as he wants depending on the level of service provided by the other.

The Expression of the payoff of the user and service provider is as follows: [23]

$Payoff^{user}$ = Personalization – Privacy Risk
= -User Data2 + Personalization * (1 + Control Effort)
$Payoff^{provider}$ = User Data - (1 – Privacy Risk)
= User Data2 + User Data - (1 + Personalization * Control Effort)

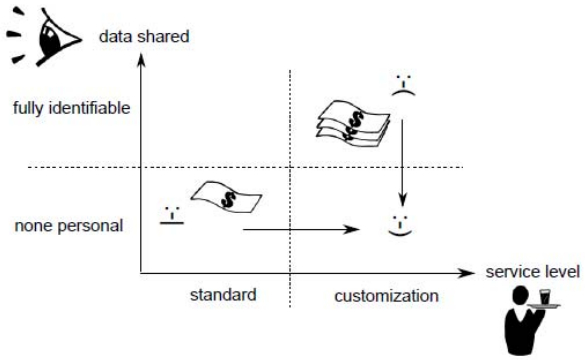

Fig. 3. Proposed Framework to assess business models for privacy management [23].

Another grave issue pertaining to consumer privacy in the mobile world is that of service providers selling user information and preferences to third parties. This is due to the fact that service providers provide some services to the user for free due to the unwillingness of the consumer to pay for these services. Through these services, service providers gain personal information about the user. These services include applications that perform location based services.

Service providers are inclined to sell the user data to obtain higher incomes while on the other hand regulatory forces push the service providers to provide good services to the user without jeopardizing their privacy [23].

In the year 2000, companies referred to as "Infomediaries" and were believed to be the absolute key to users having some power over their information being publicized [23].

The job of an infomediary is creating a link between consumers and vendors. They are the agents, keepers and brokers of the consumer's information and protect their privacy. But ten years later, there were no real Infomediaries protecting consumer privacy available.

Most business do not have any real motivation to furnish users with a comprehensive privacy feature since it doesn't really help them distinguish from other services [23]. On the other hand, most users do not seem to be antagonized over the issue neither are they requesting for it. This should be a matter of social responsibility and businesses should pioneer the privacy movement rather than wait for customers to request for it [23].

V. Privacy Concerns in Online Financial Transactions

In recent years, due to the incessant evolution of IT systems, there have been several new technologies in the offering of financial services. A large number of people now opt for electronic means of payment while gradually abandoning the old payment systems [24]. This however has brought it with considerable privacy and security concerns for both the payment intermediaries and consumers likewise

[24].

A payment system involves intercommunication between various entities.

The Central Bank in each country plays a vital function in the maintenance of payment systems by laying down the modalities and ensuring actions that would guarantee and improve the systems stability [24]. Also they have to ensure the stimulation of consumers trust and the protection of itself from illegal usage [24].

As with other methods of crime, to be able to properly appraise the lengths to which internet and advanced payment systems can be appealing to a person laundering money or bankrolling terrorism, it is first required to take a look at the pros and cons of such endeavors. Points that should be looked into include the convenience, availability, invisibility of operators and the ease of transferring funds between countries whilst being able to exploit legalities [24]. Electronic money provides a certain degree of advantages to people involved in money laundering as it stands as a substitute for banking and legal money contribute to the system in terms of ease of access, efficiency, speed and instant accessibility [24]. But also on the other hand, it can also help to boost money laundering and other financial crimes; therefore there is a need to revisit the systems of controls currently being used [24].

Most payment systems can be traced back to the source as every transaction keeps a record even if it is only for a short while. But these records can be hidden, deleted with different types of encryption, even possibly retrace it to another source other than the originating source. In the compromise between privacy protection and the needs of the public, there is still the need to decide where to draw the line between storing user's information and controlling the system and users. [24]

VI. E-Governance and Privacy Concerns

Electronic governance enables their citizens to conduct government transactions online which can be a relief as it can be tasking going to the office physically [25]. Citizens can renew their license, pay taxes etc online. But citizens are sometimes unwilling to provide their personal information online because they do not trust that their information is safe in this manner [25].

There are several perceived internet privacy risks associated with in the e-government environment such as reputation, improper access, error, collection, third party certificates, and secondary use [25].

a. The reputation of a web page determines the risk levels associated with it and the development of trust with the site and the users. Users are more inclined to trust well known organizations they "feel' they can trust [25].
b. Improper access is a situation when people that do not have the proper clearance to access certain information have undue access to this information. This is the reason for the concerns of individuals when refusing to disclose personal information because they do not trust the organizations to give priority to protecting their information [25].
c. Errors may be done on purpose or by mistake whereby an unauthorized user has access to another person's information. The users also fear that the organization may not be doing much to ensure the safety of their private information [25].
d. Collection is the collation of personal data required to perform a transaction. Doubts here arise from the citizen not trusting the agency to have the capability to collect this information and properly store the information securely [25].
e. Third party certificates are highly regarded by users and increases levels of trust of a website. There are various seals that are popular on secure websites; therefore users feel more protected if these third party seals are available on a website asking for their personal information [25].
f. There is also the issue of unauthorized secondary use of user's data. This is the case whereby information is collected for a certain purpose and then later used for something else. This may occur if agencies exchange data without the users' permission [25].

In terms of e-governance, these are the main fears and risks associated with information privacy [25].

VII. What Security Measures can be taken to Implement Consumer Online Privacy

Companies should put in place stringent security measures to ensure consumer online privacy. These measures could be in different types. Measures both general & pervasive should inform an organizations security policy. Some of these measures are outlined below: [26]

A. Education

- Establish regular interactive sessions where employees are taught efficient security procedures.
- Websites can be used as a medium of communication in teaching employees online etiquette.
- Customers should be reminded to update relevant antiviral & antispyware software [26].

B. Security Department

- There should be an autonomous security department with full fiscal control of itself.
- A 24/7 service desk in which identity theft and other related activities can be reported by customers.
- The office of the chief security officer who will be responsible for online security should be created.
- A security policy should be created and fully implemented.
- Internal auditors could be engaged as an extra measure [26].

C. Constant Monitoring

- Agencies could be engaged to monitor activities on their websites.
- Following transactions, notification alerts can be sent to the customer probably via e-mail & preferably by SMS. This will enable the customer react immediately in the event the transaction is illegal [27].
- Internal auditors could also be engaged.
- Monitoring of traffic, carrying out a traffic flow analysis

and tracking of transactions would enable knowledge on who has access to the database [27].

D. Security Tools

- Sensitive data should be encrypted using strong algorithms that cannot be broken. Unencrypted financial information should be closely guarded.
- Efforts should be made to assist users in identifying spoofed websites by making use of SSL & multi-layer security.
- Dual authentication procedures can also be implemented e.g. making use of session tokens for users.
- Email correspondence should be characterized by digital signature.
- The webpage interface the user uses could be affixed with an image selected by the user during initial registration. This would help the user distinguish it from a spoof site.
- Fraud detection can also be achieved using hitherto successful data mining tools [28].
- Automated artificial intelligence measures can also be taken to detect subtle changes in online patterns & behavior [29].

VIII. Cybercrime Impacts on Confidence of Consumers

Fig. 1 below intends to illustrate relationships among the impacts of identity theft, use of information, and invasion of privacy as a result of cybercrimes and the counter e-security measures and policies taken to promote consumer confidence [30].

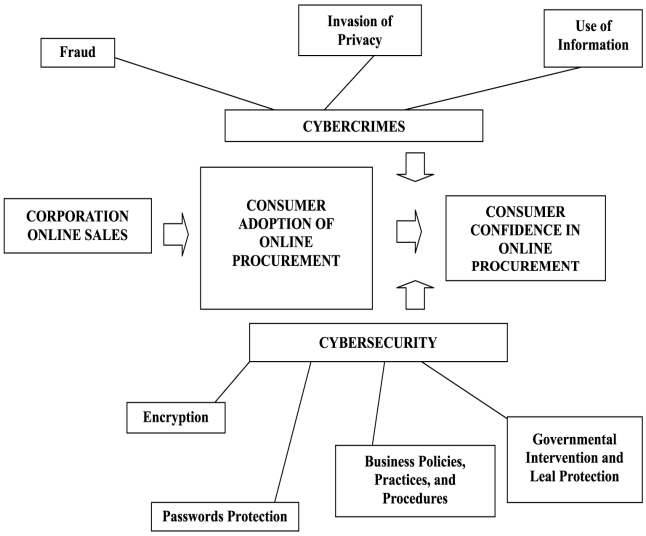

Fig. 4. Proportioning forces connected with cybercrime and cyber security [1].

IX. Discussion

The word Consumer online privacy is an ongoing concern in the internet age; this concern is present in almost every sector as has been analyzed above. Government and Private agencies responsible for the custody of consumer information have the duty to keep this information private and not disclose to any third party without permission from the consumer. However the consumers still do not feel that they are totally protected. Something Customers are actually unaware of when surfing websites is that it is not just their personal information that is being collated but also their choices as regards to preferred web pages and choices when shopping online.

Some agencies deem it their inalienable right to make use of information supplied them by their consumers as has been illustrated in the cases of the mobile industry whereby some mobile operators share consumer information with third parties to make profit without prior consent from the users. This can also be said for social networking sites where users information can be made public, some of this networking sites now have features that allow the user to hide their data and only have it exposed to the people they want but not everyone is aware of this functionality as the default setting actually leave you exposed. Identity theft, online fraud, invasion of privacy and loss of trust are some of the backlashes that emanate from consumer privacy compromise. Also in the Financial Sector, privacy is of major concern as people who do unlawful transactions online can through various methods of encryption reroute the records of their transaction to a third party who probably has no idea of what has gone down. This way an innocent individual could get blamed or involved in some illegal acts probably because he was careless with his information himself or his financial institution does not have very good security measures in place. There have been several cases celebrated and understated of this breaches. Various arguments have been raised on the legality or otherwise of the use of information obtained by breaching consumer privacy. One may look at the current riots taking place in the UK, it is widely acknowledged by the London Metropolitan police that some rioters coordinate their activities using social networking tools like Twitter, instant messaging application on the blackberry and post some of their activities on Facebook. Deputy assistant commissioner Stephen Cavanaugh confirmed officers were looking at the websites (Twitter and Facebook) as part of investigation into widespread looting and rioting. It is suggested that they would achieve this by finding out personal details of suspects on these social Networking sites. There are also arguments on whether this form of evidence would be admissible in court on prosecution given the nature by which they were obtained.

The level of privacy that an individual perceives when browsing a web page is what determines their online behavior. As long as a customer "feels" that a website is secure enough depending on the level of security certificates present, he will have no hesitations in revealing his personal information on that webpage and possibly even re-using that same service.

X. Conclusion

This paper has examined consumer online privacy as an ongoing concern in the 21st century, as more users are added to the internet and more sites go live so does the risk of consumer online privacy breach increase. Privacy issues has been examined in government, mobile and financial sectors as these mediums require users to provide some level of personal information if not all as would be in the case of the

financial institutions. All these organizations need to see the need and importance of creating a real and functional security policy within their organizations and on their websites if they are to get their consumers full trust and thus attract new customers. Although some of the fears expressed by the consumers are not actually real fears, they could be categorized as perceived fears because these are concerns that the users just imagine could also happen such as the issue of trust. To address these perceived fears of consumers, organizations need to work on building a higher level of trust with their customers as these is the only way to avert those fears. This can be done by clearly stating and showing the customers what exactly they are doing to ensure the safety of their information and keep them abreast of new development in that field. This way the users would feel that the organization does care about their privacy and safety of their information. Also a feature could be provided that would allow users determine how much of their private information is available publicly. We have looked at the possible threats to consumers which include passive attacks like phishing, phreaking, skimming and pretexting. Also examined were the effects of consumer privacy being compromised such as identity theft, invasion of privacy and use of information. The various security measures that could be used to curb these various attacks have also being outlined to include proper education of staffs of organization on proper security procedures and also to inform consumers by putting up notice on the organization website. Having a dedicated security department for online security in an organization is necessary to ensure effective and dedicated attention to these threats. Effective monitoring of activities on an organizations website and employing necessary security certificates on a website are also methods outlined in this paper as a means to manage consumer online privacy. Consumer online Privacy is of very important concern to the consumers even to those who don't realize their information may have been leaked to a third party. Organizations should make this matter a priority so as to instill a higher level of trust in their customers and thus also increasing their own sales. Consumer Online privacy should not be looked down on by organizations, government and even social Networking Sites as these could result in loss of huge sums of money to the customers and also result in loss of trust in the particular organization which could possibly lead to their downfall if not properly managed. Proper Management of consumer online privacy would lead to increased trust in the organization by its clients who could translate into increased profitability. It's a WIN/WIN situation. The factors that can be seen as actual consequences to the improper handling of consumer data would be that of hackers and phishers trying to get information from organizations websites with the intent of causing harm and stealing data to be sold in the "black market". To combat these issue, organizations would still have to ensure that they have adequate and efficient safety practices on their websites as they would be held responsible if a customer's data gets used for anything illegal. And these security measures would need to be reviewed and upgraded frequently because as an organization is working hard to have efficient security services, at the same time, unauthorized users are also working hard to break these barriers. Therefore, maintaining proper security measures for online businesses is an endless practice as the 'attackers" Basically an individual's idea of online privacy depends on their perception of the amount of some items present during their online experience that have no adverse results. These items include: Freedom, security, supervision and intimacy to express themselves online.

REFERENCES

[1] P. Waldmeir, "Should Americans exchange privacy for security?," The Straits Times, 2001

[2] A. F. Westin, "Privacy and freedom," *Journal of Social Issues*, vol. 59, Issue 2, pp. 508, 1970.

[3] D. V. Geeta, "Online identity theft – an Indian perspective," *Journal of Financial Crime,* vol. 18 , no. 3, pp. 235-246, 2011.

[4] W. Lusoli and R. Compano, "From security versus privacy to identity: an emerging concept for policy design?" info, vol. 12, no. 6, pp. 80-94., 2010.

[5] W. Stallings. "Network Security Essentials," Prentice Hall, Third Edition, pp 366, 1999.

[6] J. Wirtz, "Causes and consequences of consumer online privacy concern," *International Journal of Service Industry Management,* vol. 18, no. 4, pp. 326-348, 2001.

[7] A. D. Miyazaki and S. Krishnamurthy, "Internet seals of approval: Effects on online privacy policies and consumer perceptions," *Journal of Consumer Affairs*, vol. 36 Issue 1, pp 28 – 49, summer 2002.

[8] M. J. Culnan and G. R. Milne, "Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices" *Journal of Interactive Marketing,* vol. 18, Issue 3, pp 15-29, summer 2004.

[9] S. C. Shih, "E-enterprise security management life cycle," *Information Management & Computer Security*, vol. 13, no. 2, pp. 121-134, 2005.

[10] K. B. Anderson, E. Durbin, and M. A. Salinger, "Identity Theft," *Journal of Economic Perspectives,* vol. 22, no. 2, pp. 171–192, Spring 2008.

[11] A. M. Antonopoulos, "The black market for identity," Network World, Available: http://www.networkworld.com/columnists/2007/091007-risk-reward.html , September 11, 2007.

[12] M. –L. Francisco, L. –M. Teodoro and S. –F. Juan, "How to improve trust toward electronic banking," *Online Information Review*, vol. 34, no. 6, pp. 907-934, 2010.

[13] J. Woo, "The right not to be identified: privacy and anonymity in the interactive media environment," *New media and Society*, vol. 8, no. 6 pp. 949-967, 2006.

[14] A. Acquisti, A. Friedman, and R. Telang, "Is there a cost to privacy breaches? An Event Study," Twenty Seventh International Conference on Information Systems, Milwaukee and Workshop on the Economics of Information Security, Cambridge, UK, 2006.

[15] C. E. Wills and M. Zeljkovic, "A personalized approach to web privacy: awareness, attitudes and actions," *Information Management and Computer Security*, vol. 19, no. 1, pp. 53-73, 2011.

[16] A. Acquisti, "Privacy and security of personal information: Economic incentives and technological solutions," The Economics of Information Security, 2004.

[17] H. B. Wijnholds, and M. W. Little, "Regulatory issues for global e-tailers: marketing implications," *Academy of Marketing Science Review,* vol. 1, no. 9, 2001.

[18] E. P. Becerra and P. K. Korgaonkar, "The Effects of trust beliefs on consumers' online intentions," *European Journal of Marketing,* vol. 45, no. 6, pp. 936-962, 2011.

[19] L. Carter and A. McBride, "Information privacy concerns and e-government: a research agenda," *Transforming Government: People, Process and Policy,* vol. 4, no. 1, pp. 10-13, 2010.

[20] International Telecommunication Union, "Cyber Security guide for Developing Countries," ITU, Edition 2007.

[21] R. Mekovec, "Online Privacy: overview and preliminary research" *Journal of International Organizations Studies,* vol. 34, no. 2, pp. 195-209, 2010.

[22] J. J. Wirtz, M. O. Lwin, and J. D. Williams, "Causes and consequences of consumer online privacy concern," *International Journal of service industry management,* vol. 18, no. 4, pp. 326-348, 2007.

[23] R. Bonazzi, B. Fritscher, and Y. Pigneur, "Business model considerations for privacy protection in a mobile location based context," Proceedings of the Second International Workshop on Business Models for Mobile Platforms. IEEE, 2010.

[24] G. Merlonghi, "Fighting financial crime in the age of electronic money: opportunities and limitations," *Journal of Money Laundering Control,* vol. 13, no. 3, pp. 202-214, 2010.
[25] M. Brown, and R. Muchira, "Investigating the relationship between internet privacy concerns and online purchase behavior," *Journal of Electronic Commerce Research,* vol. 5, no. 1, pp. 62, 2004.
[26] R. E. Goldsmith, B. A. Lafferty, and S. J. Newell, "The Impact of Corporate Credibility and Celebrity Credibility on Consumer Reaction to Advertisements and Brands," *Journal of Advertising,* vol. 29, no. 3, pp. 43, 2000.
[27] K. L. Keller, J. W. Alba, and J. W. Hutchinson, "Branding perspectives on social marketing, advances in consumer research," *Association for Consumer Research,* vol. 25, pp. 299-302, 1998.
[28] M. S. Featherman, A. D. Miyazaki, and D. E. Sprott, "Reducing online privacy risk to facilitate e-service adoption: the influence of perceived ease of use and corporate credibility," *Journal of Services Marketing,* vol. 24, no.3, pp. 219–229, 2010.
[29] R. Cullen, "Culture, identity and information privacy in the age of digital government," *Online Information Review*, vol. 33, no. 3, pp. 405-421, 2009.
[30] A. D. Smith, "Cybercriminal impacts on online business and consumer confidence," *Online Information Review*, vol. 28, no. 3, pp. 224–234, 2004.

Zainab B. Nurudeen (NIGERIA - 26/05/ 1983), B.Sc (Computer Science), University of Ilorin, Kwara State, Nigeria. She is currently undergoing her MBA in Multimedia Management at Limkokwing University of Creative Technology, Malaysia. She has about 4 years working experience in Information Technology and services. She also holds a Cisco Certified Network Associate (CCNA) certificate. She worked with a major Telecommunication vendor, Huawei Technologies for 2.5 years in the capacity of a Network Design and Sales & Product Manager. Previously she had worked with a Government agency involved in e-Governance, National e-Government strategies for 2 years as the Assistant Webmaster.

Rashad Yazdanifard (IRAN - 22/05/ 1982), M.A. (Industrial Management), Shahid Beheshti University, Iran. He has done his Work completion seminar in his PhD in the field of Marketing at Multimedia University, Malaysia and he is currently in final stages of completing his Viva. His Major Field of Study is online marketing and E commerce.He has been lecturing in several Universities for 4 years and since 3 years ago till now, He has been lecturing in Limkokwing University of Creative Technology in Center Of Post Graduate Studies and Faculty of Information and Communication Technology located in Cyberjaya, Malaysia. UCI (Unity College International) was his previous Employer .He has done more than 80 Conference and journal Papers by now in his academic career. The majority of papers are around the fields of E-Commerce, Electronic Marketing, General Management and Human Resource Management.

Abdullahi A. Nasiru (NIGERIA - 02/12/ 1980), B.Eng (Mechanical Engineering), University of Ilorin, Kwara State, Nigeria. He is currently undergoing his MSc. in Computer Networking at Limkokwing University of Creative Technology, Malaysia. He has about 5 years working experience in Networking. He is currently on study leave from the Lagos state University, Lagos, Nigeria where he has been the Network Administrator and Head of the Network support department for 4 years. He also holds a Cisco Certified Network Associate (CCNA) certificate and the Cisco Certified Academy Instructor (CCAI) as he is also in charge of the Cisco Networking Academy resident at the Lagos State University.