Internet Privacy: A Survey of Cyber Abuses and Policy Improvements in Ghana

[1,2]Alimatu-Saadia Yussiff, [1,2]Abdul-Lateef Yussiff, [2]Said Jadid Abdulkadir

[1]Department of Computer Science and Information Technology, University of Cape Coast, GHANA

[2]Department of Computer Science and Information Sciences, Universiti Teknologi PETRONAS, MALAYSIA

E-mail: asyussiff@ucc.edu.gh, ayussif@ucc.edu.gh, jadid86@gmail.com

ABSTRACT

The exponential growth of the Internet and its ability for instantaneous communication anywhere and anytime has already revolutionized the individuals' ways of life, organizations and businesses activities. Simultaneously, the internet has equally provided us with advanced tools and techniques to carryout unlawful activity. It is often common of late to hear of privacy infringement, identity theft and internet fraud that would never have materialized without the internet. This research employed mixed method approach to investigate the current level of knowledge the internet users in Ghana have on internet privacy and the abuses that can occur, understand the current policies as well as Ghanaians perceptions and finally to propose a policy recommendation to help curb and or eliminate the growing occurrences. This information will help to expose the loopholes and also act as a necessary tool to draw attention to the Government on the need for effective policy reforms on internet privacy abuse. It was realized that too much time has been wasted and so much damage has been done but to avoid further occurrence of the abuse and also to ensure the security of internet users in Ghana, the issue of internet privacy abuse has to be addressed urgently.

Keywords*: Internet; Privacy; Abuse; Internet Privacy; Spam; Spim; University Of Cape Coast, Ghana; Universiti Teknologi PETRONAS.*

1. INTRODUCTION

The internet is a network of networks with common address space and common communication protocol. It's an invention that has significantly changed human interaction and help advance development at a phenomenal rate due to its ability to make available much needed information at a click of a button. The whole concept of internet privacy came about as a result of individuals, businesses and organizations placing personal and confidential information on the internet.

Ghana is a country with a steady economic environment; it is a peaceful country that can be considered as a developing nation. It adopted the use of the internet in the early 1990's and has since seen a steady rise in the use of the internet by its citizens [1]. The internet is currently used by many elites in every aspect of human interaction such as email, chatting, social networking, searching, storing of information and for online purchasing. Although, internet in the country is still at its permeation stage, it has however been linked with many cases of internet fraud especially cases involving credit or debit card theft, stealing of personal information through phishing, spoofing, 419 email scam, online dating scam, false advertisement or marketing among others. These have led to the blocking of e-business, travel websites, paying and transferring money from Ghana. Internet privacy and cyber-crimes are intertwining terminologies that is difficult to separate one from the other. One can hardly talk about internet privacy without mentioning the cyber-crime.

The inadequacy of policy implementations to help curb the menace, as well as the proliferation of mobile devices with broadband connections as well as the attitude and behaviour of users and many other factors have led to the issues of the alarming rate of internet privacy abuse in Ghana.

As at 2011 the estimated number of internet users in Ghana was at 3,479,359.93 out of 24,658,823 million people. This is less than fifteen per cent of the population. Figure 1 shows the graph of internet users in Ghana based on the percentage of the population. Internet users' statistics was obtained from the ITU report [1].
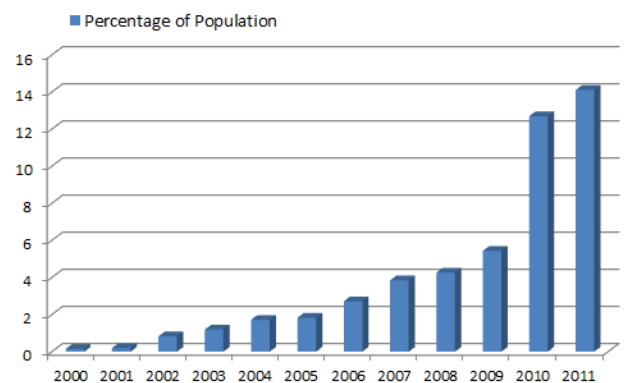

Figure 1: Percentage of Individual Using the Internet

Out of the vast number of internet users in Ghana, only a tiny minority of them are aware of the term, "internet privacy". Most of them just use the internet without knowing its consequences. Some of them do not even see spam mails as a negative thing and are quite excited to receive them even though they did not subscribe to them. Some also care less about reading through the privacy agreements on websites. They are much too interested in the capabilities of the internet and have not been made aware of the dangers. This is largely due to the fact that Ghanaians have not yet been introduced properly to internet business and as such the populace use the internet for more information or entertainment related activities than business activities that would require secure connections.

Thus, most internet users have in one way or the other experienced a breach on their privacy either in the form of spam mail, identity theft, phishing and many others. Internet privacy abuse has grown to become a prevalent occurrence all over the world and more so in developing countries like Ghana. These raise the questions;

- What can be done to improve the state of Internet privacy in Ghana?
- How can Ghanaian benefits from internet business?
- What is the plan of government in ensuring the security of internet users?
- What is the government's policy on this issue?
- Can there be a transformation in the country's image as a bad image as a hotspot for internet crime?
- Are Ghanaians aware of the necessity of internet privacy and security?
- What can Internet service providers, business owners and individual users do to improve internet privacy, security and its awareness in the country?
- What policies can be proposed to the Ghanaian government?

The main aim of this research is therefore to investigate the issue of internet privacy abuses in Ghana, understand the current policies as well as Ghanaians perceptions and finally to propose a policy recommendation to help curb and or eliminate the growing occurrences.

2. RELATED WORK

A. Aspects of Internet Privacy Abuse

Internet privacy is the ability of the individual, businesses or organization to control information about themself when transacting businesses and or transmitting data or information online. It include having full control over the type or amount of personal information that is being revealed online as well as those who can access those information [2]. It also include freedom from intrusion and freedom from surveillance [3].

Internet privacy abuse has taken on two forms, generally classified as harmless abuse and malicious abuse [4]. Harmless abuse can be classified as attacks that are not targeted on a person usually a marketing stunt or email marketing. There are also the false promotions to attract people's attention to a particular website for commercials and publicity. One classic example of harmless abuse is mild spamming usually used for advertisements and evangelism or information spreading, it doesn't usually cost the receiver a lot of harm except a few seconds wasted checking and deleting it. [4]. Either harmless abuse or not, it's a trespass and infringement on people's privacy.

Malicious or harmful abuses are far more dangerous and costly than harmless abuses. They are usually premeditated and are carried out strategically. They include identity theft, social engineering to get details of individuals for malicious purposes. Examples include, bank statement theft, bank account infiltration and many others [4]. Spams are also being used by criminals for fraudulent activities like kidnapping, collecting ransom and stealing. One example is the case of Robert Alan Soloway in 2007 who used "millions of zombie computers to distribute spam [5]" across the United States, he was later prosecuted and charged for identity theft, wire and email fraud among others [5].

B. Common Internet Privacy Abuse Attacks in Ghana

Some attacks that Ghanaians are susceptible to, include phishing, a fraudulent technique or method of gaining access to people and organizations personal and or private information online. This is mostly carried out by sending faked email that look like legitimate such as from ones family, friend a bank, or credit card company requesting verification of information and warning of some dire consequence if it is not provided. Secondly, social engineering, the act of manipulating people to reveal personal and confidential information is currently being used by youth of Ghana. This has become so rampant that a popular name, "Sakawa" has been given for such act in Ghana. [6].

Email Spoofing is another attack experienced by Ghanaians. This involves getting access to and altering the email address of companies and individuals to impersonate them for mostly illicit activities. An example is to receive email that look legitimate from a bank or credit card company with links to update account information. This is all an attempt to breach a person's privacy and obtain their personal secrets for malicious activities. Such malicious activities include; bank fraud, identity theft, credit card theft, social security benefits theft and many others.

In addition, as online payment is slowly becoming more accepted in Ghana, credit and or debit card fraud is on the rise. Scammers have started employing physical tactics such as theft, using service employees (waiters,

waitresses) to obtain people credit and debit card numbers of card users. Some are even using advanced method such generating debit and credit card numbers [6].

Online fraudulent activities became rampant in the Accra Metropolis mostly through the internet café terminal. The Marketing Manager of Busy Internet, Mr Francis Ahene-Affoh, was said to have reported in 2004 through an interview that Internet fraud is a problem to all internet café operators in Ghana. He identified online shopping as the primary means of defrauding people. He further explained that the management of Busy Internet has tightened up security as a means of combatting internet frauds. The management of Busy Internet does not allow online shopping unless the facilities users identify themselves to be those they claimed they are. He disclosed that a number of arrests have been made and the culprits were handed over to the police [7].

C. Security Agencies and Organizations on Internet Crimes and Abuses in Ghana

Currently, it is the Ghana Police Service, especially CID (Criminal Investigations Department), and the BNI (Bureau of National Investigations) handle internet fraud cases. The good news is that there is currently a breakthrough in attracting internet users' attention to the internet safety crisis in Ghana. In a workshop that was organized by the Internet Society (ISOC), Ghana chapter, in Accra in May 2013, the participants were sensitized on internet governance, standards and on cyber security. Participants were also made aware that an online gateway had been installed, but yet to be inaugurated [8]. It is our hope that more of such training and workshops be organized through out the ten regions of Ghana to sensitize Ghanaians.

D. Ghanaian Legislation to Prevent Internet Abuse Offences and to Punish Offenders

Examples of such legislation in Ghana include; the Data Protection Act, the Companies Act and the Financial Service Act. The Data Protection Act is the only one related to privacy in any manner and still it involves more of data theft or misuse policies than internet privacy protection. Also, in 2008 the government of Ghana passed the Electronic Transactions Bill to protect private rights of Internet users and owners' websites [9].

E. Cases of Internet Abuse in Other Countries

Researchers have reported on different cases of internet abuse and privacy infringements all over the world. There are people on the internet who use anonymous servers to avoid responsibility for controversial remarks. Hiding your identity is a matter of personal choice and also sometimes a matter of security. Cases of harassment and abuse are under ascendance even though stringent measures are being employed by organizations. A survey published in 2011 by an independent research and consultancy company, BuddeComm, revealed that banks in some Africa countries specifically, Uganda, Tanzania,

Kenya Zambia and Rwanda lost about 245 million US dollars in 2011 to cyber fraud [9].

In the United States of America, the Internet Crime Complaint Center (IC3) in 2012 received 289,874 internet abuse complaints from consumers with an estimated loss of $525,441,110 which was an increase of 8.3% from that of previous year. The internet abuse complaints from consumers include online sale of vehicles they do not own, email scam, hit man scam, citadel malware to extort money from internet users, intellectual property right and trademark infringement [10].

A Brazilian bank's outsourced ATM maintenance supplier had inserted data stripping devices to copy pin numbers and other bank data from cards used in the machines [11]. In another development, A retailer in Colombia recounted how corrupt employees had, in collaboration with criminal elements, installed devices at the register to copy data from cards swiped there and sell it for the production of cloned cards [11]. Also, One Caribbean bank, a leading issuer, explained how members of its own IT department had downloaded card holder identities from its own computers [11].

3. METHODOLOGY

The research was conducted using mixed-method approach by employing survey method to collect quantitative data, semi-structured interviews, participant observation, and documentation analysis for qualitative data.

A. Data Collection

First, secondary search and analysis were made through internet research, books, newspapers, radio and television news to gather in depth knowledge about concepts and issues on internet privacy and abuse. Second, questionnaire instrument was design making up of 16 questions to investigate how Ghanaians understand the concepts of internet and internet privacy. It was also used to investigate if Ghanaians were aware of internet privacy abuse and what their reactions are. We further had to know whether the government of Ghana had policies in place to protect their citizenry or rules to prosecute and punish internet privacy offenders. Finally, it was used to obtain the views of internet users that are aware of privacy and its abuse and vice versa in Ghana, and to explore the main reasons behind those abuses.

The questionnaire was designed keeping in mind both, internet semi-expert users and casual internet users. Most of the questions were therefore open-ended. Some of the questions are general for all respondents and other address a specific group of participants. Questionnaire distribution was chosen because it is an effective way of acquiring information from multitudes of people without the researcher being present. Also this provided an anonymous way of seeking answers from people who did not want to be mentioned or known.

B. Population

The population under consideration is Ghana. Due to its vast area and travel constrains of the researching group, the study was limited to four of its ten regions, namely; Ashanti, Greater Accra, Central, and Western regions. These regions were selected according to their development rate and the technological advancement in that area.

C. Sample Size

The total numbers of questionnaires distributed in the four regions were three hundred and forty-one (341). Out of this total, ninety-eight (98) questionnaire were distributed in Greater Accra region; in Central Region one hundred and two questionnaires were distributed (102), in Ashanti region eighty-one (81) questionnaires and in Western Region sixty (60). Although 341 questionnaires were distributed, only 104 questionnaires were returned. Most respondents did not complete all the questions and as such the data set for analysis varied according answered questions. Only the first question (What do you understand by internet) seemed popular and was answered by all respondents. The data was then analysed using SPSS and Microsoft Excel statistical tools.

4. RESULTS AND DISCUSSIONS

A. Results

i. Internet Usage

Table 1 is a representation of the internet usage in the four regions that were surveyed, encouragingly a larger percentage of them (55.4%) are proficient while (44.6%) are average internet users who are mostly unaware of exactly what they are doing. This statistics shows that out of the total number of Ghanaians surveyed on the use of internet, many of them are aware of the internet and its capacity to build you up or bring you down. This calls for the need to educate the populace on various measures and solutions to the internet privacy issues and abuses. As this statistic shows that with just a little prompting and effort, the government can easily educate the internet populace on the dangers and effects of internet abuse.

Table I
Internet Usage in Four Regions of Ghana

Region	Total Questionnaires Distributed	Novice Users	Proficient Users
Greater Accra	98	39	59
Ashanti Region	81	28	53
Central Region	102	64	38
Western Region	60	21	39
TOTAL	**341**	**152**	**189**

ii. Internet Privacy Awareness

Table 2 and Fig. 2 show the analysis of the internet privacy literacy in Ghana categorized by age. The analysis shows that most people (63.5%) are aware of internet privacy and the majority of the people who are aware of it are people below the age of 21. The remaining 36.5 are unaware of what is termed internet privacy.

This statistics answers our research question on internet privacy literacy in Ghana as most youth are aware of it. This would in turn solves the problem of how and who to target the education to among the population. This knowledge will also allow the research team to know where to focus more energy in the development of research solutions that will focus more on the adult. Informing and educating adult on issues relating to internet abuse will go a long way to improve Ghana future ambitions of being a safer place for internet users. Educating the youth more will be an added advantage since they are the future of this nation.

Table II
Internet Privacy Awareness by Age

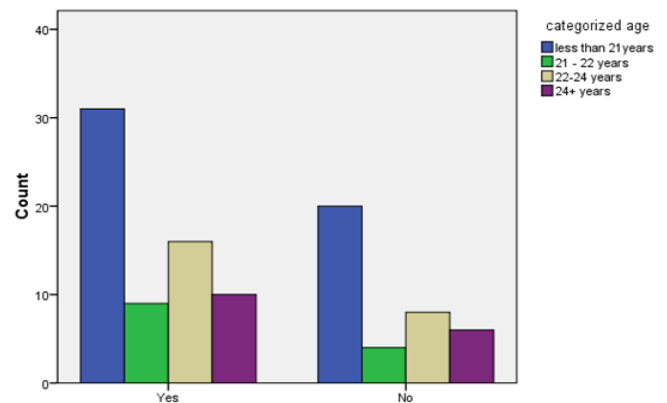| Age (Years)	Yes		No		Total	
	Freq.	**%**	**Freq.**	**%**	**Freq.**	**%**
< 21	31	47	20	52.6	51	49
21 - 24	25	37.9	12	31.6	37	35.6
≥ 24	10	15.1	6	15.8	16	15.4
Total	**66**	**100**	**38**	**100**	**104**	**100**

Fig 2: Internet Privacy Awareness by Age

iii. Compromise of Internet Privacy Abuse

Table 3 illustrate the analysis of the internet privacy abuse in Ghana categorized by age. It answer the question, do you feel your privacy have been compromised in any occasion? This analysis shows that most of the respondents (67.7%) believe they have been victims of internet privacy before. The analysis also shows that most

Ghanaians need to be educated about internet privacy abuse and how to avoid them.

Table III
Internet Privacy Abuse Categorized by Age

Age (years)	No		Yes		Total	
	Freq.	%	Freq.	%	Freq.	%
< 21	12	40	34	53.9	46	49.4
21-24	12	40	21	33.3	33	35.4
≥ 24	6	20	8	12.8	14	15.2
Total	30	100	63	100	93	100

iv. *Knowledge of Internet Privacy Laws Currently Applicable in the Country*

Majority of the respondent (89.7%) as shown in Table IV are unaware of any internet privacy laws in the country. This answers our research question, do you know about internet privacy laws currently applicable in the country? This is reflective of the situation in the country as there are no vivid internet privacy laws currently applicable in Ghana. This is therefore a call on the government and ministry of information to enact policies and regulations and make sure they are implemented to the maximum.

Table IV
Internet Privacy Law Awareness in Ghana Categorized by Age

Age (years)	Yes		No		Total	
	Freq.	%	Freq.	%	Freq.	%
< 21	6	60	41	47.1	47	48.4
21 - 24	3	30	33	37.9	36	37.1
≥ 24	1	10	13	15	14	14.5
Total	10	100	87	100	97	100

Fig. 3 illustrate that most people (89.7%) do not believe they have had any internet privacy abuse. It was realised during the questionnaire distribution phase that most people were clueless about the different types of internet privacy abuse that existed. To them internet privacy abuse is all about '*Sakawa*'.
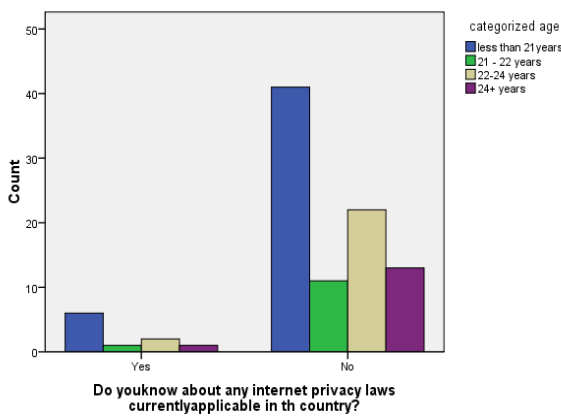

Fig. 3: Awareness of Internet Privacy Laws

v. *Do current laws in the country protect the user against privacy abuse?*

48 out of 76 respondent representing 63.2% as illustrated in Table V and Fig. 4 believe that the current laws in Ghana do not offer the user any protection against internet privacy abuse. This calls for the necessity of law and policy to be enacted and implemented to safe guide and protect internet users since the internet has come to stay.

Table V
Influence of Current Internet Laws on Privacy Protection categorized by Age

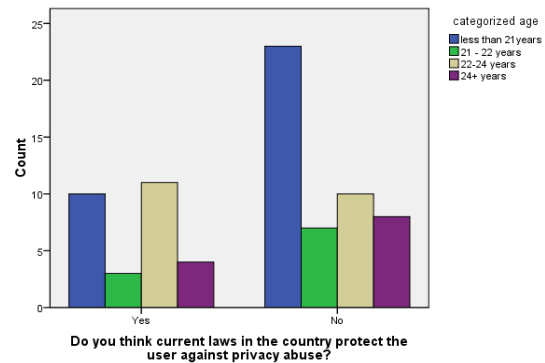|	< 21 years		21 - 24 years		≥ 24 years		Total	
	Freq	%	Freq	%	Freq	%	Freq	%
Yes	10	30.3	14	45.2	4	33.3	28	36.8
No	23	69.7	17	54.8	8	66.7	48	63.2
Total	33	100	31	100	12	100	76	100

Fig. 4: Influence of Current Internet Laws on Privacy Protection categorized by Age

B. *Findings*

It is eminent from the results above that adequate policies have not been put in place to promote internet security thus internet business cannot be fully exploited in Ghana owing to the fact that insecurities exist amongst the populace and businessmen. In addition, it was realized that Ghanaians are not fully aware of the concepts of internet privacy and security. Some do not even know when their privacy have been compromised or measures to take to avoid any occurrences of the menace. The most interesting fact found during the analyses was that the age range of the active internet users are the youth and they are most often impacted by internet privacy abuse or are themselves involve in it.

Finally, most of the respondents are of the view that the current laws in Ghana do not offer the user any protection against internet privacy abuse. They are also certain that there is currently no law on internet privacy abuse.

5. **POLICY RECOMMENDATION FOR GHANA**

The internet as network of networks is borderless. Thus, issues of internet abuse cannot be fought by Ghana alone. It should cooperate with other countries to deal with privacy infringements, fraud, spam, spim and other issues related to the internet at the local, national, regional and international levels. All stakeholders in internet provisions

and users from national and international level must be involved in this movement. Information and Communication Technology institutions must be established to train cyber and internet security experts in "system administration, security audit, forensic investigation, information security and software development to deal with the future challenges of cybercrime" [9]. In addition, lawmakers must be well trained and sensitized to help implement legislation that addresses internet crime at all levels [9].

Also, effective polices must be established to guide all internet users, providers and stakeholders and to investigate their activities. Businesses have a responsibility to use security tools and monitor their systems to prevent attacks from succeeding. Developers have a responsibility to develop with security as a goal.

Awareness of internet privacy abuse and its effects is tantamount to the success of controlling this abuse or completely eradicating it. It can also be carried out by the use of the media such as FM and TV stations in both local and English languages, posters distribution, bill board adverts, seminars and workshops. All these will go a long way to achieve this goal. A lot of sensitization will be needed to let the general public understand fully the concepts of internet privacy, internet security and ways to alert the appropriate authorities.

Users should also take time to carefully read out privacy agreements on websites they subscribe to. They can also help out by reporting fraudulent persons they come into contact with on the internet to help build a database of suspicious sites and persons for internet security. Users should be educated on internet dangers to ensure that all privacy settings are enabled on their personal computers before using the internet. This education should include;

- User configuring the security of internet services they subscribe for.
- Users checking for secure connections (https) before uploading information.
- Users checking that the logging off process is complete before leaving their systems at public places like cafes, airports, and hospitals.
- Users keeping their personal information confidential such as their passwords.
- Users have a responsibility to ask questions and educate themselves on the tools to maintain security (personal firewalls, anti-virus and anti-spyware, security setting on social media sites).

Internet Service providers (ISPs) as a body can implement stricter firewall configurations to prevent network packet sniffers from having access to sensitive information being sent across the network, they could also prevent access to dangerous websites that steal user information for malicious conduct by blocking access to such websites. Some more specific suggestions and recommendations Internet service providers include:

- To secure their bandwidth and use of encryption for the confidentiality of packets transfer over their network.
- To provide and have latest technology such as, high technology authentication systems.
- To be aware that whenever a person signs in, the person has entered into agreement or contract with them and all efforts must be made to protect the integrity of the users.
- To not sniff and or infringe on people privacy themselves.

Other countries like the USA, UK and Canada have the Internet Crime Complaint Centre (IC3) and legislations in place. China has centralized censorship to prevent proliferation of harmful information and Dubai has measures in place to prevent illegal downloading and copyrighting. Ghana can adopt such measures as well.

6. CONCLUSION

Internet privacy is a right and as such it has to be earned and safeguarded. It is earned by becoming an internet user and it is guarded by consciously reminding oneself that even though the internet is a big and wonderful tool for global communication, it is also a big and dangerous monster for all kinds of criminal acts so be watchful, do not intentionally do anything that will jeopardize the safety of our own or others personal information online.

This research has brought to light the Ghanaian mentality and approach to the internet and its vices. Ghanaians do not really care that much about internet security because they do not use the internet for safety critical operations like e-commerce transactions. The concept of e-banking has just been introduced into the country and it is still in a somewhat pilot stage because only few people actually opt for it. This is an indication that most Ghanaians do not trust the internet. These phenomena have to be changed with good policy and legislative instrument to back all internet users and improve the image of the country.

Also the government of Ghana is responding slowly to the global movement that is pushing most world economies electronic with internet trading, marketing, advertising, and banking pushing small economies to grow since it requires small capital to implement. This type of trade is exactly what Ghana needs to propel itself to a new level in development. The government has to realise that before e-commerce can take root in Ghana and produce any meaningful development they need to get the citizenry to trust the internet or at least assure them that any information they provide on the internet is safe and well guarded.

Given the monumental dangers surrounding internet privacy abuse in the world, and the deterring image of Ghana in the e-business, effective policies should be put in place in Ghana to at least greatly reduce the risks involved in the practice if not completely eradicate this menace. This would be a gradual process as the saying goes *Rome*

was not built in a day but certain immediate steps have to be taken in order to ensure it becomes a reality. Proper awareness and sensitization of the general public and policy makers in the country will go a long way in educating and informing everyone about ensuring their privacies are not infringed upon on the internet and to aware of the various steps to be taken to ensure their privacies are being protected.

The sole purpose of this research was to investigate the internet privacy abuse situation in Ghana and recommend policy improvements. The greatest policy improvement that can happen to Ghana as far internet privacy abuse is concerned is awareness. Awareness by the people, but most importantly awareness by the government, until the government gets the fact that internet privacy is a major issue that has to be tackled to redeem Ghana's internet image we will not excel in the new, exciting and very lucrative world of e-commerce.

The good news is that there is currently a breakthrough in attracting internet users' attention to the internet safety crisis in Ghana. In a workshop that was organized by the Internet Society (ISOC), Ghana chapter in Accra in May 2013, the participants were sensitized on internet governance, standards and on cyber security. Participants were also made aware that an online gateway had been installed, but yet to be inaugurated. This forum indicated that the government has seen the extent that internet development and security can impact positively on the majority of the economy of a nation.

REFERENCES

[1] I. T. Union, *The World in 2012: ICT Facts and Figures,* *www.itu.int/en/ITU-D/Statistics/.../Individuals_Internet_2000-2011.xls*: ITU, 2012.

[2] Wikipedia. (2013, June 3rd). *Internet Privacy* Available: http://en.wikipedia.org/wiki/Internet_privacy

[3] S. Baase, "A gift of fire," 2003.

[4] D. Mann and M. Sutton, ">> NETCRIME More Change in the Organization of Thieving," *British Journal of Criminology,* vol. 38, pp. 201-229, 1998.

[5] J. A. Ophardt, "Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield," *Duke L. & Tech. Rev.,* p. i, 2010.

[6] K. Owusu. (2010). *Internet Fraud: Scams made for Ghana.* Available: http://233.com.gh/posts/2010/tech/real-tech/internet-fraud-ghana-scams/

[7] A. Mail. (2004). *Internet Fraud On the Ascendancy in Accra.* Available: http://www.modernghana.com/news/62110/1/internet-fraud-on-the-ascendancy-in-accra.html

[8] G. MMA. (2013). *Workshop on Internet Governance Opens in Accra.* Available: http://www.ghanamma.com/2013/05/workshop-on- internet-governance-opens-in-accra

[9] H. O. Quarshie and A. Martin-Odoom, "Fighting Cybercrime in Africa," *Computer Science and Engineering,* vol. 2, pp. 98-100, 2012.

[10] I. C. C. Center, "IC3 2012 Internet Crime Report," 2013.

[11] Kroll, "Kroll Global Fraud Report," 2009.