

This item was submitted to [Loughborough's Research Repository](#) by the author.
Items in Figshare are protected by copyright, with all rights reserved, unless otherwise indicated.

Nigerians' perceptions of personal data protection and privacy

PLEASE CITE THE PUBLISHED VERSION

PUBLISHER

BCS / © The Authors

VERSION

AM (Accepted Manuscript)

PUBLISHER STATEMENT

This work is made available according to the conditions of the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0) licence. Full details of this licence are available at:
<https://creativecommons.org/licenses/by-nc-nd/4.0/>

LICENCE

CC BY-NC-ND 4.0

REPOSITORY RECORD

Adelola, Tiwalade, Ray Dawson, and Firat Batmaz. 2019. "Nigerians' Perceptions of Personal Data Protection and Privacy". figshare. <https://hdl.handle.net/2134/20241>.

Nigerians' Perceptions of Personal Data Protection and Privacy

Tiwalade Adelola, Ray Dawson, Firat Batmaz

Department of Computer Science, Loughborough University,
Loughborough, United Kingdom

Abstract

The influx of E-commerce into Nigeria has resulted in individuals shopping online and sharing personal information about themselves and their family, friends and colleagues. A survey and interviews were conducted to gain an initial understanding of attitudes about privacy among Nigerians and their understanding of E-commerce data protection and privacy. It was found that Nigerians are generally aware of the dangers of online data theft, but their concern was focussed almost exclusively on the theft of financial data. They did not trust the government to protect their data with any effective legislation or law enforcement, but they were happy to submit their financial information through a bank's website. However, it was found that Nigerians had little concern about other, non-financial information, which leaves the population vulnerable to the theft of other forms of personal and private data.

1.0 Introduction

This paper is an analysis of public opinion surveys on public understanding and knowledge of data protection and privacy in Nigeria. Data protection and privacy gain social importance as technology and data flows play an ever greater role in shaping social structure [1]. Despite this, understanding of public opinion on these issues is clearly lacking. The paper firstly considers the understanding of disclosing and disclosed personal information. The general perception of purchasing online is investigated and how concerned Nigerians are about providing personal details when purchasing online. This is followed by the public's perception on current data protection practices in Nigeria. The level of privacy concern about organisations' use of personal information, policies on sharing information with third party organisations, and the level of trust in government and private companies are considered. Finally the public's level of awareness of the repercussion of bad privacy, data protection practices and individual self-protection methods are considered.

2.0 The Conceptual Framework and Hypothesis

Cultural values and privacy perceptions differ from country to country. These varying values exert a significant influence over how privacy is respected and treated in a given country. This, in turn, determines what data protection approaches a country adopts or if a country has effective data protection [4,5]. Factors, such as the political changes in a country, economic priorities and the public's perception of personal information and its protection can affect how privacy is viewed which then influences the adopted privacy policy.

Hypotheses one: The current views of privacy are focussed mainly on financial aspects and knowledge of other aspects of privacy protection is insufficient.

Some nations may or may not be overly concerned about the need for data protection to protect their citizens or corporations. This is notable in the case of developing African nations, such as Nigeria, that lack privacy protection legislation [7]. Studies have shown that regulatory responses usually occur in reaction to a growing level of information security concern within the masses [4, 6]. Nigeria is known for its high level of cybercrime, so many Nigerians are becoming aware of the dangers on putting credit/debit card details on just any website [7]. This has prompted many e-commerce website to adopt the pay by delivery method [8]. This method provides peace of mind as no bank or card details are compromised. However, is there still the danger of personal identifiable information misuse?

This paper supports the suggestion that the current views of privacy are focussed mainly on financial aspects, and knowledge of other aspects of privacy protection is insufficient.

Hypotheses two: The public generally show higher levels of trust in private bodies rather than in the government to protect their privacy interest.

The government has endorsed draft guidelines on data protection and cyber security in the past, but there is yet to be any legislation and there is no immediate prospect on anything being passed as a law [9]. According to a survey by transparency international [10], 73% of the Nigerian population believe that the Nigeria legislative and parliamentary body is opaque and corrupt. Nigeria, being a developing economy, is striving to provide the basic infrastructure of a steady supply of electricity, good roads and transportation, health, education services and postal and telecommunication networks [11]. Considering this, it is safe to say that the enactment of a working data protection policy would not be the government's priority.

Hypothesis three: Many people are starting to use the Internet, but the vast majority of the Nigerian population that use the Internet are unaware of the dangers associated with it

One of the repercussions of bad data protection and privacy practices is identity theft. Apart from companies or government protecting the privacy interest, there should be awareness of self-protection methods. The lack of user awareness of these methods could lead to identity theft

3.0 Research Method

The study included a survey and brief interview. Mixed method was used in this study as both quantitative and qualitative approaches were used. The methodology used for the study is explained below

3.1 Survey

A survey was developed with the goal of collecting opinion-based information from individuals who reside in Nigeria. Web and paper-based collection channels were used to make completion of the survey as convenient as possible.

Links to the survey website (qualtrics) was distributed via social networks (Facebook, Twitter and Blackberry Messenger). The paper-based questionnaires were distributed on a university campus and in private companies. 74 completed surveys were obtained. Two of the respondents who didn't answer more than the demographic questions were eliminated, leaving 72 responses.

Table 1: Description of Respondents' Characteristics.

	N=72
	Percentage
Sex	
Male	51%
Female	49%
Age	
<20	23%
20-29	41%
30-39	24%
40-49	8%
<50	4%
Education Qualifications	
PhD	3%
Master's Degree	20%
Bachelor's Degree	42%
Undergraduate	34%
School Certification	1%
Primary School	0%

To keep the survey form short, only those items crucial to the research objectives were included. Hence, key items focused on individual perceptions about

institutions that collect and use personal information and general perceptions of personal information. More focus is made on younger and educated Nigerians. The main reason for this is that based on previous studies, the majority of those who regularly use the internet are within the age of 15-24 and have post-secondary education [10] and may well have different views on and approaches to the disclosure of personal information to those who rarely use the internet. They are classified as digital natives: 'young people born during or after the general introduction of digital technology' [11]. Just 10% of the respondents were above the age of 40 and all respondents were educated at least to the level of an undergraduate. Table one summarises the demography of the sample. The survey tool (quatricks) was used to analyse the results.

3.2 Interviews

Brief one-on-one interviews were conducted to get an in-depth and personal view of the individual. 10 of the survey respondents were chosen at random and interviewed. No personal information (name, email address, etc.) that would identify any individual was collected. The interviews contained questions that provided more detailed information about views on providing personal information while performing online transactions, on government's involvement in data protection and on website policy documents. The interviews took place when respondents were answering or finished answering the survey questions and were conducted in Lagos. All interviewees were between the ages of 18 and 39 (5 were in their thirties, 4 were in their twenties and 1 was below the age of 20).

An opportunistic approach was used to determine which of the participants were chosen for the interview.

4.0 Survey Analysis

This section presents the analysis of general perceptions of purchasing online, comfort levels sharing different types of data online, trust in businesses and government, and third party information sharing. The results are reported as percentages calculated after removing those surveys that had missing answers for the particular question

4.1 Importance of Personal Information

The disclosure of personal information seems to have become an increasingly common part of everyday life. It can be open and deliberate in some cases, in exchange for services or unintentional and hidden, for example when behaviour is being tracked through websites, mobile phones or credit cards [3]. One of the aims of the survey and interviews was to determine what people consider personal information that they would not easily disclose. This section examines Nigerians' disclosure of personal information, what they consider to be personal information, and how they feel about disclosing their personal information online.

4.1.1 Information considered as personal

Respondents were asked how comfortable they were providing specific information to web sites. There are significant differences in the comfort levels for different types of information. Respondents were most comfortable sharing their gender, email address, religion, Facebook address and full name with web sites. They were least comfortable sharing bank account details, passport number, Health and medical history, Debit/credit card number, and annual income.

There is also a clear relationship between online purchasing and regarding financial information as personal. 61% of those who shop online say this information is personal, compared with 90% of those who do not purchase online.


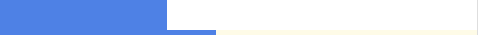


Table 2: Which of the following information is personal to you that you and would NOT like to share when making a transaction online?

#	Question	Always feel comfortable	Sometimes feel comfortable	Never feel comfortable
1	Annual Income	22%	12%	66%
2	Age	45%	33%	22%
3	Bank account details	2%	21%	77%
4	Credit/Debit card details	10%	34%	56%
5	Email address	73%	18%	9%
6	Facebook address	69%	15%	16%
7	Full name	64%	25%	10%
8	Gender	87%	4%	9%
9	Health and medical history	15%	21%	64%
10	Home address	11%	39.13%	49.28%
11	Land line/mobile phone number	29%	54%	16.%
12	Photograph	9%	35%	56%
13	Marital Status	54%	30%	16%
14	Occupation	60%	24%	16%
15	Passport number	4%	21%	75%
16	Religion	75%	16%	8%

4.1.2 Disclosing personal Information during online transactions

All respondents were asked if they performed transactions online. The general finding is that there is still a bit of reservation about performing transaction online with nearly half the respondents only occasionally or never doing so.

Table 3: Do you buy things or perform transactions online?

Answer		%
Always		18%
Very Often		35%
Occasionally		45%
Never		2%
Total		100%

Interestingly, many of the respondents are not bothered about providing personal information when performing online transactions. About half of the respondents (54%) are occasionally bothered, 15% are never bothered, 20% are often bothered and just 11% of the respondents were always bothered about providing personal information. Respondents were also asked their preferred mode of payment. The pay on delivery method (55%) had the highest percentage closely followed by credit/debit card (42%).


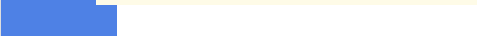


4.2 Protection of Personal Information

Companies holding personal information may sometimes use it for a purpose other than that for which it was collected. Surprisingly a larger percentage of respondents were not concerned about this. The survey asked questions to determine their opinions on e-commerce websites collecting and processing their information.

4.2.1 Concern about the uses of Personal Information

When performing transactions online, most e-commerce websites require customers to provide and save their personal information on their website. Respondents were asked if they ever wondered about the use of their information on websites. According to the results shown in Table 3, interestingly, the majority of the respondents only occasionally or never wondered about the use of their personal information

Table 4: Have you ever wondered what happens to the personal data provided on a website?

Answer		%
Always		20%
Very Often		24%
Occasionally		44%
Never		11%
Total		100%





4.2.2 Possible Accessibility of Personal Data by Third Parties

There are no requirements for Nigerian web sites to post privacy policies. However, as privacy policies are becoming increasingly expected on commercial web sites around the world, Nigerian web sites are beginning to post them.

Respondents were asked whether they usually read privacy statements on the Internet. 41% of the respondent wouldn't bother reading the privacy statement and nearly one third more (30%) of the respondents only did so occasionally.

Although many of the respondents wouldn't bother reading websites' privacy statement, as shown in table 5, the majority of the respondents were always or very often concerned when they received e-mails from organisations with which they had never shared their information.

Table 5: Does getting spam emails from third party organisations with which you have never shared your data bother you?





Answer		%
Always		38%
Very Often		20%
Occasionally		37%
Never		6%
Total		100%

4.2.3 Trust in E-commerce companies

To understand the level of trust Nigerians have in E-commerce websites, respondents were asked if they verified authenticity of a website before they purchase online.

Table 6 shows that while the majority of the respondents are cautious enough to check the company's authenticity most of the time, a significant minority of more than a third, never or rarely do so.

Table 6: Do you verify authenticity of a website before giving your personal information?

Answer		%
Always		44%
Very Often		17%
Occasionally		29%
Never		10%
Total		100%

4.2.4 Trust in Government

Respondents were asked if they trusted the government to fully handle data protection and privacy issues. A general lack of trust in the government on these issues is shown in the results with fewer than one in 6 agreeing that the government could be trusted, with none strongly agreeing, whereas nearly half disagreed or strongly disagreed.

Table 7: Government can generally be trusted to look after privacy interests.

Answer		%
Strongly agree		0%
Agree		16%
Neither Agree nor Disagree		36%
Disagree		31%
Strongly Disagree		17%
Total		100%

4.3 Awareness

Everywhere we use information services; we leave traces making it possible for anybody who is interested in collecting and analysing our personal data. Hacking with the purpose of stealing confidential data is a very common cyber-attack known today. Once a user's account is compromised, there could be ramifications such as identity theft. A hacker can gain access to very confidential information such as bank account and credit/debit card details, home address etc.

4.3.1 Identity theft awareness

The respondents were asked if they were aware of identity theft and its repercussion. Three quarters of the respondents were well aware of identity theft. However, the majority (66%) gained this awareness through media such as television

Table 8: Are you aware of identity theft and the repercussions?

Answer		%
Yes		75%
Not sure		21%
No		4%
Total		100%

4.3.2 Self-Protection Techniques

Respondents were asked about awareness of some common self-protection techniques. Table 9 shows that the most common was deleting cookies (44%), but more than a third were not aware of any techniques at all.

Table 9: Which self-protection techniques are you aware of?

Answer		%
Deleting cookies		44%
Altering browser settings		25%
Providing false information		25%
None		38%
Others		3%

5.0 Interview Analysis

Brief interviews were used in conjunction with the questionnaire to aid better interpretation of results. The interviews created an avenue to ask for further clarification of certain issues and assisted in gathering additional information that were not captured by the survey.

5.1 Disclosing Personal Information Online

The interviewees were asked if they felt comfortable providing their information when performing transactions.

All of the interviewees regularly use the Internet and perform online transactions. Six out of the interviewees had no problems providing their personal information when performing transactions. Four indicated they had no issues disclosing their information if they are familiar and trust the website. All the interviewees stated that debit/credit card details are the information they feel least comfortable providing when purchasing goods and services online.

5.2 Reading website policies

Eight of the interviewees indicated that they never bother to read website policies and two said they read them on occasion. The most prevalent reasons for not reading them are that they are lengthy and difficult to understand. Only one of the interviewees said they read website's return policy and reviews on the website to verify the authenticity.

5.3 Trust in Government

The interviewees were asked if the Nigerian government could be trusted to handle privacy and data protection affairs. A brief explanation about the current data protection approach in the United Kingdom was given for more understanding. Six out of the interviewee stated that the government cannot be fully trusted to handle the nation's privacy and data protection needs. Three indicated that they can be trusted and one wasn't sure. One of the interviewees added that they are sure that the government has or is planning to have a data protection system but they are also sure that it won't be in any way effective or reliable. Another of the interviewees stated that the government simply isn't ready to fully handle privacy issues but probably would be some time in the future. All of the interviewee agreed that the website owners and the bank should be responsible for protecting customer's information

6.0 Conclusion

This study was undertaken to understand the attitudes of Nigerians about privacy through a written survey and interviews.

Most of the survey respondents felt their financial information (bank account details) was the most important personal information. It was found that most of the interviewees felt least comfortable providing their credit/debit card details when performing transactions online. This could be the reason why the pay-on-delivery payment option is becoming the most popular payment option in Nigeria. However, it is important to note that many of the respondents were still comfortable with the credit/debit card payment method. This could be because the banks solely manage the online payments of E-commerce websites in Nigeria with these websites linking to the bank's website to handle the payment rather than handling the transaction themselves. The banks in Nigeria are a relatively effective institution and seem to command the trust of the population. This supports the first hypotheses that state that the current views of Personal Identifiable Information privacy are focussed mainly on financial aspects and knowledge of other aspects of privacy protection is insufficient. It is apparent that the public places value on the idea of privacy and data protection, but the only real concern is for financial information.

Most of the respondents were either indifferent or totally disagree that the government can be trusted to look after the citizens' privacy interests. This distrust may have originated from the government's inability to enact any legislation. Generally, the bank and to a certain extent, the e-commerce website, are perceived as being the major regulatory body in terms of Nigerian E-commerce. This fully supports the second hypotheses that state that the public generally show higher levels of trust in private bodies rather than in the government to protect their privacy interest.

There is a good awareness of identity theft amongst respondents. Although it was very clear that this awareness was gained mainly from the media, especially through television. Most of those that were aware of self-protection techniques were aware that they could delete cookies, but many were not aware of any preventive techniques. The awareness of identity theft exists, but there seems to be a lack of appreciation of the dangers of this type of theft and that leaves the population very vulnerable. This supports the third hypothesis that states that many people are starting to use the Internet, but the vast majority of the Nigerian population that use the Internet are unaware of the dangers associated with it. In general, a majority have accepted the disclosure of personal information is necessary for e-commerce but appear to be minimally concerned about providing information unless financial information is concerned. The advantage of there being little concern about companies misusing their personal information is that this could lead to a rapid growth of E-commerce. However the downside is that their lack of concern could mean that the Nigerians are vulnerable to their information being misused.

The recommendations of this paper are, therefore, that steps should be taken to make the Nigerian people more aware of their vulnerability to theft of their personal and private information. Clearly the Government of Nigeria have not got

the time and resource to put in place effective legislation to protect the citizens against identity theft, but in any case, even if they did so, the population would not trust them to enforce this legislation. However, this research has found that the media has provided a means to educate Nigerians on the existence of identity theft, so this channel could be further exploited to make Nigerians realise that identity theft could be a serious danger and to show them how to protect themselves. This would then help protect the population until effective laws and enforcement is possible.

7.0 References

1. D. Hallinan, M. Friedewald and P. McCarthy, "Citizens' perceptions of data protection and privacy in Europe," *Computer Law and Security Review*, no. 28, pp. 263-272, 2012.
2. S. J. Milberg, S. J. Burke, H. J. f Smith and E. A. Kallman, "Values, personal information privacy and regulatory approaches," *COMMUNICATIONS OF THE ACM*, vol. 38, no. 12, pp. 65-74, 1995.
3. R. Sarathy and C. Robertson, "Strategic and Ethical Considerations in Managing Digital Privacy," *Journal of Business Ethics*, p. 111–126, 2003.
4. V. Rudraswamy and D. Vance, "Trans border data flows: adoption and diffusion of protective legislation in the global electronic commerce environment," *Logistics Information Management*, vol. 14, pp. 127-136, 2001.
5. Wolf Park; Digital Jewels, "The 2014 Nigerian Cyber Threat Barometer Report," 2014. [Online]. Available: <http://www.wolfpackrisk.com/portfolio/2014-nigerian-cyber-threat-barometer-report/>. [Accessed 25 June 2014].
6. C. Chiejina and E. Soremekun, "Investigating the Significance of the 'Pay on Delivery' Option in the Emerging Prosperity of the Nigerian e-commerce sector," *Journal of Marketing and Management*, vol.5, no.1, pp. 120-135, 2014.
7. F. Akinsuyi, "Data protection for Nigeria, The time is now," 2007. [Online]. Available: <http://www.datalaws.com/common/pdf/Article02.pdf>. . [Accessed 3 February 2015].
8. Transparency International, "Nigeria," 2013. [Online]. Available: <http://www.transparency.org/gcb2013/country/?country=nigeria>. [Accessed 30 June 2014].
9. K. Uma and F. Eboh, "Corruption, economic development and emerging markets: evidence from Nigeria," *Asian Journal of Management Sciences and Education*, vol. 2, no. 3, July 2013.
10. Broadcasting Board of Governors, "Contemporary Media Use in Nigeria," 2014. [Online]. Available: <http://www.bbg.gov/blog/2014/04/30/bbg-research-series-contemporary-media-use-in-nigeria/>. [Accessed 3 February 2015].
11. TNS Opinion & Social, "Attitudes on Data Protection and Electronic Identity in the European Union," Special Euro barometer, Brussels, 2011.

