AFRICA UNIVERSITY

(A United Methodist Related Institution)

TECHNOLOGICAL ADVANCEMENT : A CAUSE FOR SECURITY AND PRIVACY CONCERNS

BY

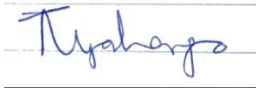
TATIANA NGAATENDWE NYANHONGO

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THEREQUIREMENTS FOR THE DEGREE OF BACHELOR OF SCIENCEHONOURS IN COMPUTER INFORMATION SYSTEMS IN THE COLLEGE OF BUSINESS, PEACE, LEADERSHIP AND GOVERNANCE

2023

DECLARATION

I, NYANHONGO TATIANA, hereby declare that this proposal for Honors in Computer Information Systems submitted to the College of Business Peace Leadership and Governance at Africa University has not been submitted previously for any degree at this or another university. It is original in design and in execution, and all reference material contained therein has been duly acknowledged.

NYANHONGO TATIANA 

Student's Full Name Signature (04/05/23)

LOVELY TEMBANI FUNDISI 

Main Supervisor's Full Name Signature (04/05/23)

COPYRIGHT

Abstract

Data protection is a vital tool to the development of any country. Certain challenges pose a threat to data protection in developing countries although the same challenges are evident in developed countries. For instance, technological advancement in information technology has challenged the existing mechanisms of data protection. Other threats to data protection as identified in this paper include inappropriate legislation, inadequate internet regulations, unethical computer users in the office, computer system mal-function, hardware failure, power blackouts and power failures. Certain remedies are necessary to counteract the challenges. Some of the remedies presented include internet regulation for users and internet service providers, computer ethics education and training among users, cross-border harmonization of laws on data protection and enforcement procedures, response to and preparing for power blackouts/power failures, response to system and hardware failures and introduction of national youth development forums and self-employment initiatives. A conclusion is drawn from the challenges and the remedies discussed with great emphasis being laid upon curbing data crimes in the office work atmosphere, business atmosphere and stressing the need for strengthening the current legislation and enforcement procedures on data protection.

Key words: Threats, Legislation, Computer Ethics, Remedies, Data Crimes

TABLE OF CONTENTS

DECLARATION ***2***

COPYRIGHT ***3***

ABSTRACT ***3***

TABLE OF CONTENTS ***5***

- ***CHAPTER 1 INTRODUCTION*** ***1***

1.1 Background 1

1.2 Statement of the Research Problem 2

1.3 Research Objectives 3

1.4 Research Questions 3

1.5 Assumptions 4

1.6 Significance of the Study 5

1.7 Delimitation of the study 6

1.8 Limitation of the study 6

- ***CHAPTER 2 REVIEW OF LITERATURE*** ***7***

2.1 Introduction 7

2.2 ICT Advancement and Its Benefits in Our Modern Life 7

2.3 Conceptual framework. 8

2.4 Summary of Literature Review 10

- ***CHAPTER 3 RESEARCH METHODOLOGY*** ***11***

3.1 Introduction 11

3.2 Research Design 11

3.3 Population and Sampling Procedures 12

3.3.1 Population of the study 12

3.3.2 Sampling Procedures 13

3.4 Data Collection 14

3.5 Data Analysis 16

3.6 Ethical Considerations 17

CHAPTER 4 DATA PRESENTATION , ANALYSIS AND INTERPRETATION

4.1 Introductiony.....9

4.2 Data Presentation Analysis.....9

4.3 Analysis Of Interviews And Focus Group.....10

4.3.1 Topics Discussed During Interviews And Focus Group.....10

4.3.2 Findings Of Overall Results.....10

4.3.3 Summary.....11

CHAPTER 5 SUMMARY , CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction.....12

5.2 Discussion.....12

5.3 Conclusions.....13

5.4 Recommendation.....13

5.5 Suggestions For Further Research.....14

- **CHAPTER 1 INTRODUCTION**

This research is focusing on impact of Security and privacy concern due to technology advancement. This research will deal with privacy and security in Internet-based information systems as study will be done with the main focus being the advance in technology. Increased interconnectivity among nodes or end user devices and systems enabled by networking technologies has boosted the scale and scope of risks and dangers related to personal and other sensitive information. Due to these advancements in technology, there is so much misuse of information which often leads to breaches in security and intrusions into privacy.

1.1 Background

Human beings value their privacy and the protection of their personal sphere of life. They value some control over who knows what about them. They certainly do not want their personal information to be accessible to just anyone at any time. But recent advances in information technology threaten privacy and have reduced the amount of control over personal data and open up the possibility of a range of negative consequences as a result of access to personal data. In the second half of the 20th century data protection regimes have been put in place as a response to increasing levels of processing of personal data. The 21st century has become the century of big data and advanced information technology (e.g. forms of deep learning), the rise of big tech companies and the platform economy, which comes with the storage and processing of Exabyte of data.

At the same time, the meaning and value of privacy remains the subject of considerable controversy. The combination of increasing power of new technology and the declining clarity and agreement on privacy give rise to problems concerning law, policy and ethics. Many of these conceptual debates

and issues are situated in the context of interpretation and analysis of the General Data Protection Regulation (GDPR) that was adopted by the EU in spring 2018 as the successor of the EU 1995 Directives, with application far beyond the borders of the European Union.

The focus of this article is on exploring the relationship between information technology and privacy. We will both illustrate the specific threats that IT and innovations in IT pose for privacy and indicate how IT itself might be able to overcome these privacy concerns by being developed in ways that can be termed "privacy-sensitive", "privacy enhancing" or "privacy respecting". We will also discuss the role of emerging technologies in the debate, and account for the way in which moral debates are themselves affected by IT.

1.2 Statement of the Research Problem

The art of technological advancement is embraced by all nations including developing countries. Today, the world is like a village where people share information at the same time but in different parts of the world over the internet. Developing countries venture into new technologies without understanding the implications and the legal frame works under which the technologies operate. According to the 28th International Conference of Data protection and Privacy commissioners (2006), the technological pace keeps accelerating while the legal pace remains particularly slow. For this reason, developing countries may not effectively deal with crimes committed over the internet or in the office work environment. Spammers for instance, may send spam over the internet with little or no knowledge of users in developing countries. Although these countries may have laws on data protection, these laws are general in character and may not apply in crimes like spamming. Palfrey (2005) explains that, some countries use existing laws of general application to fight crimes like spam. Unfortunately, these laws miss their target.

A lot of progress has been made in discovering new knowledge in the field of information and communication technology. Some of the new knowledge and advancements have been used destructively. For instance, hackers use their high-tech skills to change, intrude or interfere with computer networks with an intention of destroying information or making some money out of it e.g. a banking fraudulent deal. Bullesbach (2004) notes that, development and application of new information and communication technologies lead to challenges of data protection. Though new technologies in developing countries are a positive step of development, proper planning is necessary before applying new knowledge. Hackers use principles of new technologies. It should be noted that hackers may indeed be consultants in the particular firms they are working for. It means that such crimes may go undetected or can be detected after a long time.

1.3 Research Objectives

- Assess the impacts of technology Advancements in developing societies
- Analyze the socio-economic threats and privacy concerns caused by the adoption of new technology
- Determine how impacts of security and privacy intrusion can be prevented
- Examine how to enable trust for digital information and data transactions in such technology advancements

1.4 Research Questions

1. What is the impact of technological advancements in developmental society?
2. What are socio-economic threats and privacy concerns caused by the adoption of new technology

3. What preventive measure can be put in place for the impacts of security and privacy intrusion
4. What are the antecedents of trust for digital information and data transactions in such technology advancements?

1.5 Assumptions

The advances in technology, for example, the unrolling of the smart technology through digital communications has improved citizens' quality of life and well-being. In this regards, IoT technology generates vast amounts of data at any given time, which is analyzed to provide services to the general populace. In the proper implementation of these technology, a critical challenge is the violation of' privacy and security, which leads to a lack of trust and pessimism toward the services of the advanced smart technology. To ensure populace's participation, smart technology developers should adequately protect their security and privacy from gaining their trust. This article presents a comprehensive review of technology advancement in security issues and privacy. It provides a basis for categorizing current and future developments in this area and developing a thematic classification to highlight the requirements and security strategies for designing and implementing smart technology. The paper identifies current security and privacy solutions and describes open research challenges and issues. An output of this study is a systematic map of literature on the subject that identifies critical concepts, evidence, challenges, solutions, and gaps. It summarizes the findings into a body of evidence that has previously been diverse and complex.

1.6 Significance of the Study

Privacy concerns seem to come up daily in the news these days, Sometimes the technologies used by the general populace or people willingly giving information about themselves away on social media. With the current developments and advancements in technology, it seems as if no one has any privacy anymore. Willingly given or not, the formerly private information of the populace is being stored, tracked, and sold to buyers for both legal and illegal uses. Though there are many stories about compromised security and privacy concerns the general public does not seem to be worried. The significance of this study is therefore to inform the general public and organisations are the importance of information that is being just spied to other organisation.

Project Planning

Project planning is a discipline addressing how to complete a project in a certain timeframe, usually with defined stages and designated resources. One view of project planning divides the activity into these steps

	WEEK 1	WEEK 2	WEEK 3	WEEK 4	WEEK 5	WEEK 6
PROPOSAL						
INTRODUCTION						
LITERATURE REVIEW						
METHODOLOGY						
RESULTS AND DISCUSION						
SUMMARY AND CONCLUSIONS						

1.7 Delimitation of the study

The delimitations of a study refer to the scope of the research aims and research questions. In other words, delimitations reflect the choices you, as the researcher, intentionally make in terms of what you will and won't try to achieve with your study. In other words, what your research aims and research questions will and will not include. This research will focus much on young people who are actively interactive on social media as the key of their social life, finding out their level of responsibility and security awareness as there are changes and advancements in technology. The research will be guided by the objectives and research questions that were outlined above.

1.8 Limitation of the study

Research limitations are, at the simplest level, the weaknesses of the study, based on factors that are often outside of your control as the researcher. These factors could include things like time, access to funding, equipment, data or participants. This research, is so much sensitive in the sense that; most people in the sample might not be willing to provide detailed information in the process of data collection, as the researcher gather information about security and privacy corns due to advance in technology. This will therefore, impact the generalizability of your findings and therefore reflect a limitation of your study. Due to the current economic situation, the financial muscle of the researcher will be also a major limitation of the research as some tools will never be rolled out due to lack of funds. It is important to note that, availability of resources contribute to the best research output. However, the researcher might not have enough resources to do the research as planned. This as well impact the targeted output and results

CHAPTER 2 REVIEW OF LITERATURE

2.1 Introduction

In research, it is important to appreciate work that have been done by other scholars. Therefore, during the research period, information will be gathered from books, online articles and journals. This chapter provides some evidences on the actual impact of Technological advancements on modern life. Moreover, core reasons of the privacy problems, and definitions of some key concepts are discussed. The chapter presents literature reviewed by the researcher. The researcher reviewed underlying theories for technological advancement. Work done by various researchers was will be incorporated in the literature review, this will help the researcher to come up with the concrete analysis of the impacts of security and privacy concerns to the society. This chapter starts by giving a brief overview of ICT advancements, security and Data/Information privacy, this goes on explaining the threats caused by the advancements of technology on a daily operation. This then provides empirical evidence to compliment the research after which the conceptual framework is presented and the chapter is concluded by giving the chapter summary.

2.2 ICT Advancement and Its Benefits in Our Modern Life

To begin with, in order to have a broad view about OICT, it is necessary to give a prompt definition of what ICT is. ICT is an abbreviation for Information and Communication Technologies. It refers to the integration of telecommunications, computers, middleware and the data systems that support, store and transmit unified communications between systems.

Technology advancements has developed continuously in recent years. According to the International Telecommunication Union (ITU), they benchmarked development according to thr IDI

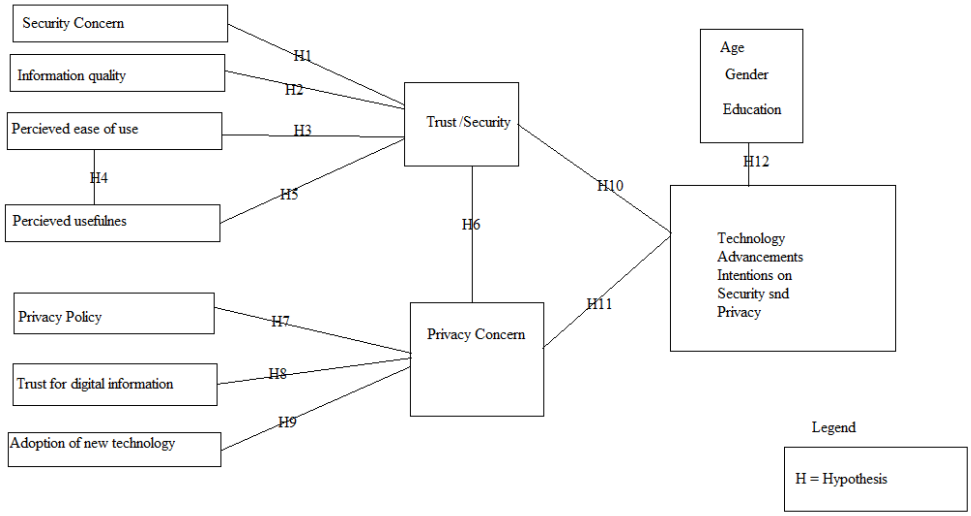
with is the ICT Development Index based on identified 11 technological indicators, grouped in three clusters: Access, Use and Skills.

2.3 Conceptual framework.

A conceptual framework plays a significant role in aiding a researcher to derive meaning from his or her subsequent findings. According to Accenture (2018), conceptual framework is a central part of the plan for negotiation to be examined, tested, studied and transformed as a result of investigation and it explains the possible connections between the variables as denoted. In a statistical perspective, the conceptual framework describes the relationship between the main concepts of a study. It is arranged in a logical structure to aid provide a picture or visual display of how ideas in a study relate to one another (Grant and Osanloo, 2019).

Based on the TAM, the researcher will develop her own model. Originally developed as a tool to estimate whether a new technology would be accepted by consumers, the TAM has since been used extensively to research the adoption of new technologies, such as online shopping according to Eneizan et al (2020) and Hyun et al., (2022. According to Davis (1989), intention to use a new technology is mostly driven by two factors: “the technology’s perceived usefulness and its perceived ease of use”.

Framework for security and privacy concern



Drivers of customers trust in the use of social media for e-retailing services

Based on the TAM and prior research on populace trust, the researcher will identify five factors as main drivers of trust: Information quality, security concerns, perceived ease of use, perceived usefulness, and privacy concerns. Information quality is defined as consumer's perceptions about accuracy and the completeness of information in the online context, Khan et al (2021). Trust in an online provider increases when consumers perceive it to be a source of reliable information Customers' willingness and ability to adopt and use new technology have been studied from a variety of theoretical perspectives, as documented in the academic literature. Customer acceptance and use of technology-related apps can be better studied using the TAM's preferred methodology out of these three options (Pal and Patra, 2021). First introduced by Davis (1986), the TAM posits that the acceptability of an information system is influenced by individuals' judgments of ease of use and usefulness. Consumer acceptance of various forms of technology can be explained in large part by TAM, which has gained strong empirical evidence

Drivers of privacy concerns

Citing from Ray et al. (2011), the researcher will identify three main factors as key drivers of privacy concerns that is to say; privacy/security policy, assurance seal, and disposition to third-party certification, these constructs have not been explored in the social media environment. The researcher will explore the drivers of privacy concerns in the context of social media, because of the huge impact of these variables on consumers trust.

2.4 Summary of Literature Review

In this chapter, the researcher appreciated the work that was done by other scholars towards the question under study to clearly outline their thoughts and thereby identifying their weaknesses or gaps. The units of privacy can be person-to-person, person-to-group, group-to-person or group-to-group (Leino Kilpi, et al., 2001). The dialectic nature of privacy refers to the fact that individuals continuously change their desire for interpersonal contact. There are two opposing forces at work at all times – one drawing individuals together, and another pushing them apart. Privacy can, thus, be viewed as a dynamic, dialectic process where the need for solitude and the need for interpersonal contact are constantly in opposition.

- **CHAPTER 3 RESEARCH METHODOLOGY**

3.1 Introduction

In this chapter, the researcher will present the research methodology that will be used in collecting and analyzing data that will collected to accomplish the research objectives. This research methodology specifies the procedures and techniques that the researcher will use in identifying, selecting, processing and analyzing information about security and privacy concern due to technology advancements in both public and private sectors with the key variables being social, political and economic concerns. The previous chapter informs the research techniques that the researcher will used in this research borrowing from similar studies as indicated in the empirical studies outlined in chapter 2.

The main sections outlined in this research that are critical for this research are the research philosophy, the research design, the research strategy, the population of the study, the sampling methods and procedures that the researcher used to come up with the actual participants who took part in the research, the research instruments, data collection methods and procedures, enhancements procedures for data validity and reliability and the research ethics observed. The last part gives the chapter summary.

3.2 Research Design

A research design sets the procedures that are critical in collection, analysis and interpretation of research findings (Bailey and Bailey, 2017). It gives the blue print for connecting the research problems with the empirical research. The research problem that triggered the research undertaking is the fact that the general populace is facing the challenge of privacy as technology is revolving now and again. Through a well-articulated research design, this study analysed the survival

strategies populace in Zimbabwe to enable the development of an effective model of survival strategies from in the cyberspace. The three possible research design forms are exploratory, descriptive and explanatory. For the purposes of this research, the researcher will use descriptive research design. Descriptive designs are more suitable in this situation as the researcher believes that rigorous statistical analysis using quantitative techniques are appropriate.

3.3 Population and Sampling Procedures

3.3.1 Population of the study

According to Curran and Blackburn (2015) target population is the whole aggregation of respondents that meet the designated set of criteria in a research. The target population for the study will encompass all workers in electronics retail sector, technology end user, government employees in Harare Central Business District. This group of people are important in the study because they are expected to have more valid information with respect to how the retailers interact conduct their businesses and the survival strategies.

A research sample refers to the elements drawn from the target population to participate in a research study. It is from these research elements research findings are attributed to the whole population (Bal naves, 2020). The reason that makes it preferable to use a sample is the fact that the population might be too large that research becomes impractical with that large population. The other reasons besides the large population include the fact that the researcher's resources might be limited that conducting a census might not be feasible. In this case, electronics retailers are scattered and are many such that including every electronics retailer were not possible. Some are even trading from their homes and could not be reached.

The researcher in this study will resort to a sample of the electronics retailers who will be readily available. However, inasmuch as using a sample sounds so justifiable, it can have its own limitations According to Mintzberg and Waters (2018) where a sample is drawn for research purposes, a sampling error is inevitable. This implies that the use of a sample will have the potential to reduce the reliability of research findings. This means that, it will therefore the duty of the researcher to strategize means of reducing the sampling error. In research, there are a number of formulae that can be used in sample size determination that are believed to reduce sampling error.

3.3.2 Sampling Procedures

There are two sampling methods, which are probabilistic and non-probabilistic methods. According to Crawshaw and Chambers (2001) probabilistic methods are techniques which gives all population elements equal chances of inclusion into the sample. These include cluster, stratified random, simple random and systematic random sampling. According to Creswell (2017) non-probabilistic methods are the techniques which result in population elements having unequal chances of being included into the sample.

These include quota, convenience, judgmental and snowballing sampling. The researcher's choice of sampling techniques shall be heavily skewed towards probability sampling techniques that will help to uphold the objectivity attribute of the quantitative research approach that the researcher should adopt. Non-probability sampling techniques have bias as the research elements are not given equal chances of participation unlike probability sampling techniques that give research elements equal chances of getting selected for participation.

In respect of the key strength of probability sampling methods of objectivity, the researcher in coming up with actual sample elements, will choose employees using random sampling technique.

The unit of analysis to be used in the current study will be drawn from the population of electronics retailers operating in Harare CBD. Simple random sampling will be chosen as it eliminate bias associated with choosing actual sample elements from a group of elements with no equal chances of being selected. As confirmed by Harkiolakis (2020) rigorous statistical analysis need to be done using randomized samples, hence random sampling technique will be applied in choosing sample elements.

3.4 Data Collection

Primary Data Collection

Data that will be collected from first-hand-experience is known as primary data. Primary According to Morris and Wood (2015) primary data is the data collected from the field for the first time in relation to the current research problem. In statistical surveys it is necessary to get information from primary sources and work on primary data. The researcher will use primary data collection to obtain the first hand information. This will be through the questionnaire, Interviews and focus groups

Questionnaire

A questionnaire is a data collection instrument consistent of a series of questions and other prompts for the purpose of gathering information from respondents. The researcher will design and administer, the questionnaire using the following steps;

- Defining the Objectives of the Study
- Define the target respondents and methods to reach them.
- Questionnaire Design
- Pilot Testing
- Questionnaire Administration

- Results Interpretation

Interview

Interviews consist of collecting data by asking questions. Data can be collected by listening to individuals, recording, filming their responses, or a combination of methods. There are four types of interview:

- Structured interview
- Semi-structured interview
- In-depth interview
- Focused group discussion

Advantages:

- Collect complete information with greater understanding.
- It is more personal, as compared to questionnaires, allowing us to have higher response rates.
- It allows more control over the order and flow of questions.
- We can introduce necessary changes in the interview schedule based on initial results (which is not possible in the case of a questionnaire study/survey)

Disadvantages:

- Data analysis especially when there is a lot of qualitative data.
- Interviewing can be tiresome for large numbers of participants.
- Risk of bias is high due to fatigue and to becoming too involved with interviewees.

3.9.2 Secondary data

The researcher will also make use of secondary data. Despite of the fact that secondary data is regarded as generic data unspecific to the research problem, the research should realise its importance and considered it useful in the study. For example, secondary data from CZI Retail Sector Survey Reports, journal articles, textbooks on SMEs and Business Management, newspapers and the internet will enable the researcher to establish the generic challenges threatening survival before getting to understand the specific challenges of electronics retail sector.

3.5	**3.6**	**3.7**
3.8	**3.9**	**3.10**
3.11	**3.12**	**3.13**

3.14 Data Analysis

Collected data by the researcher as quantitative data will be fed into SPSS version 23.0, for analysis purposes. Analysis will be expressed in form of percentages, standard deviations, mean values, analysis of variance (ANOVA) and correlation and regression. Percentages and mean scores helped to summarize the responses by indicating whether the majority have agreed, were neutral or disagreed. The standard deviations were used to show the reliability of the mean score by indicating the divergence or consistency of the respondents' views. ANOVA helped to test the significance of the correlation results. Data presentation of quantitative data was done using Microsoft Office packages of Word and Excel version 2016, in form of tables, tables, graphs and charts.

3.15 Ethical Considerations

Saunders, Lewis and Thornhill (2017) define research ethics as the appropriateness or suitability of the researcher's behavior with respect to the rights of the respondents and other research subjects. The researcher will seek for the consent of the sample elements before collecting data. By this, the researcher will liaise with the owners of the electronics shops to gain their permission to interact with them and their employees during the research period.

It is also worth mentioning that, the researcher will notify the owners of the electronics shops and their employees that they had unrestricted room to withdraw and withhold any of their input when they felt like. Further, the researcher will make sure that the participants would remain anonymous throughout the research, unless if permission will be granted to directly quote a respondent. All emails and WhatsApp chats to be used for data collection will have to be encrypted to ensure that the safety of the research participants is guaranteed. Furthermore, no participant will be given any financial nor non-financial benefit for participating, but will be appreciated verbally.

CHAPTER 4 DATA PRESENTATION, ANALYSIS AND INTERPRETATION

4.1 Introduction

Analyzing the data gathered to test the hypothesis and respond to the research questions is important for this study to be effectively completed. Data interpretation takes the form of a descriptive analysis, as was already mentioned in the chapter before.

The analysis, presentation, and interpretation of the study's findings are included in this chapter. Data analysis and interpretation are done in two stages. A quantitative analysis of the data is covered in the first section, which is based on the questionnaire's results. The second is a qualitative interpretation based on the findings of the focus groups and interviews.

The target population for the study will encompass all workers in electronics retail sector, technology end user, government employees in Harare Central Business District. This group of people are important in the study because they are expected to have more valid information with respect to how the retailers interact conduct their businesses and the survival strategies.

4.2 Data Presentation and Analysis

Frequency counts were performed on the data collected through the questionnaire. To find the maximum frequency of recurrence, the participants' answers to each individual question were summed together, that is, the number of times that a particular response occurs. The quantitative answers to the questions are then presented in percentage formats. Tabular format is used to present this analysis. In some instances, the researcher will combine two or more variables into a single table when using tables with a single variable.

4.2.1 Do you want to continue?

VARIABLE	FREQUENCY	PERCENTAGE
YES	150	75

NO	50	25
TOTAL	200	100

Questionnaires were distributed to 200 workers in electronics retail sector, technology end user, government employees in Harare Central Business District. 150 agreed to participate, however, 50 refused. Fortunately, this did not affect the results of the study.

4.2.2 What is your age range

AGE	TOTAL	PERCENTAGE
18-25	45	30
25-34	35	23.3
35-40	40	26.7
40-65	20	13.3
Above 65	10	6.7
TOTAL	150	100

The individuals' ages in each age group who participated in filling out the questionnaires are shown in this table. The proportion in this table demonstrates that there was no bias in the distribution of questionnaires to the various groups. It accurately reflects the researcher's objectivity in how the surveys were distributed. Various generations interact with technology in different ways, and as a result, they have varied worries about particular technologies and how they affect security and privacy.

4.2.3 What is your gender

GENDER	TOTAL	PERCENTAGE
FEMALE	85	56.7

MALE	65	43.3
TOTAL	150	100

This table shows that the results of the study were not influenced by gender bias.

4.2.3 What is your level of education

VARIABLE	FREQUENCY	PERCENTAGE
PRIMARY	15	10
SECONDARY	70	46.7
VOCATIONAL/ POLYTENIC/ UNIVERSITY	65	43.3
TOTAL	150	100

This table reveals that just 15 (10%) of the subjects had completed elementary school, 70 had completed secondary school, and 65 had the opportunity to complete postsecondary education. This suggests that the majority of participants are educated individuals who can read and write.

4.2.4 Do you use internet, at least occasionally

VARIABLE	FREQUENCY	PERCENTAGE
YES	150	100
NO	0	0
TOTAL	150	100

The results from the table shows that everyone who participated use internet, whether occasionally or not.

4.2.5 Do you have a smartphone

VARIABLE	FREQUENCY	PERCENTAGE
YES	150	100
NO	0	0
TOTAL	150	100

It is clear from the table that one of the most significant technical revolutions in human history is being sparked by the mobile phone. Today, there are more mobile phones in use than humans. People would prefer to eat less, according to surveys, than give up their smartphones. Those who leave their phones at home will go fetch them, but they will choose to go without their wallet.

4.2.6 Are you familiar with the term privacy

VARIABLE	FREQUENCY	PERCENTAGE
YES	150	100
NO	0	0
TOTAL	150	100

All of the people agreed that they are familiar with the word privacy. But the question is, are they aware of the impacts of technological advancements on their privacy?

4.2.7 We would like to know if any of the following information about you is available on the

Internet for others to see. It does not matter if you put it there yourself or someone

else did so.

No of respondents

VARIABLE	YES	%	NO	%

i.	Your employer or a company you work for	100	66.7	50	33.3
ii.	Your home phone number	45	30	105	70
iii.	Your cell phone number	115	76.7	35	23.3
iv.	Your date of birth	150	100	0	0
v.	A photo of you	150	100	0	0
vi.	Your home address	50	33.3	100	66.7
vii.	Things you've written that have your name on them	120	80	30	20

The observations below are deduced from this table:

Item 4.2.7 (i): 100 (66.7%) out of 150 subjects indicated that their employer or company they work for is available on the internet for others to see while 50 (33.3%) of subjects recorded that their companies were not on the internet, hence showing that most of the companies' information are on the internet. These overall figures could be interpreted to mean that more than half of the subjects (66.7%) are on the internet while only 33.3% were not.

Item 4.2.7 (ii): There are a few, that is, 30% who showed that they published their home phone, most of the subjects, (70%) indicated that they did not share their home phone number.

Item 4.2.7 (iii): 115 out of 150 participants confirmed that they published their personal phone numbers on the internet and only 35 people did not disclose their phone numbers.

Item 4.2.7 (iv and v): We see from this table that everyone, that is, all 150 (100%) participants answered that they disclosed their date of birth and photo for everyone to see on the internet.

Item 4.2.7 (vi): Only a few, (33.3%) showed that they published their home address, most of the subjects, (66.7%) indicated that they did not share their home address.

Item 4.2.7 (vii): 80% of the participants confirmed that they have posts on the internet that has their names.

From this table, one could say that the overall results seem to indicate that the majority of the participants knew that their information was available on the internet. In all the seven questions surveyed, the number of subjects showing that they knew their information was on the internet is higher than those who said they did not know.

4.2.8 How concerned are you about the availability of your private information on the Internet?

VARIABLE	FREQUENCY	PERCENTAGE
Not concerned	40	26.7
Somewhat concerned	30	20
Very concerned	80	53.3
TOTAL	150	100

The above table shows that Internet users are more worried about the amount of information that is available about them online.

4.2.9 Considering everything you know and have heard about the Internet; do you think it is possible for someone to use the internet completely anonymous- so that none of their online activities can be easily traced back to them?

VARIABLE	FREQUENCY	PERCENTAGE
YES	126	84
NO	24	16
TOTAL	150	100

This table shows that of the total sample size, 126 subjects is of the view that it is possible for someone to use the internet without publishing their true identity. This number amounts to only 84% of subjects. Only a few were not in agreement.

4.3 **Analysis of Interviews and Focus groups**

The qualitative technique was utilized to complement the results and fill in any blanks left by the questionnaire. This kind of approach appears more likely to provide more substance and offer in-depth information. In contrast to the generic understanding that comes from questionnaire results, qualitative research aims to develop a clear understanding of the issue at hand in a more nuanced manner. With this practice, it is possible to learn more about what people know as well as how they think, feel, and act. Individual interviews and focus groups were used to perform this component of the study. The data were described and analyzed, and the information was then presented in a narrative fashion. Structured interviews were used.

In this section, the findings from the focus groups and interviews with interviewees are discussed. The verbal replies they made during the focus group discussions and interviews are analyzed.

4.3.1 **Topics discussed during interviews and focus groups**

a. Why has Internet privacy become such a big issue?

The majority, if not all, of the groups the researcher spoke with indicated that the Internet has significantly altered people's lives. It altered how people study, think, work, establish values, and conduct themselves at work. Many values, including privacy, shifted as the internet grew and developed. At first, consumers could choose whom they wanted to share their information with. There were no problems with it, but over time, the internet made sharing more information than people wish to become a need. For instance, online shopping has made it necessary for you to provide your credit card information in order to make purchases. The way we exchange and receive information has changed, making privacy nearly impossible. People are very easily vulnerable due to the information they post online. Because of this, successfully committing identity theft has become incredibly simple for hackers.

a. How privacy has been redefined by technology

In the traditional meaning, privacy refers to restricting the information that others can learn about you. It indicated that no one should intrude on your area unless you give them permission to. In the early days of the internet, people thought in that way. On the internet, privacy still implies the same things even though things are changing. The difficulties we encounter online stem from our lack of awareness of the value of privacy and how to safeguard our digital life. The adoption of technical breakthroughs

will make it harder for us to protect our data. It is getting harder to disguise our data as more of us use our credit cards for online purchases and service subscriptions. It appears that we no longer have control over the information we communicate. Because of this, it has become challenging to define what privacy on the internet actually entails. Even if you do not want tracking cookies, you will have to let them monitor you since else the website you visit will not function properly. Cookies are little data files that websites place on a user's device to enable site customization. However, some cookies (known as tracking cookies) can be used to monitor a user across various websites, enabling features like ads for products a user has recently browsed on different websites. Also, despite your best efforts to maintain your anonymity, your friends' and family's online actions will ultimately reveal you. In such a chaotic environment, it is difficult to be precise about the definition of privacy on the internet.

a. **What are the effects of technological development on contemporary society?**

Depending on the situation, technology has provided a variety of choices to assist people retain their privacy. At the same time, privacy has become all but impossible due to technology. Although some tools and software can protect your privacy, they can equally be used to violate it. Invasion of privacy occurs far too frequently in modern culture, including on a national and international scale. For most people, having access to privacy when you need it is a valuable resource. Important information, like documents, account statements, and other personal data, should be accessible without having to worry about it being lost, compromised, or tapped. Your information is safer and more secure thanks to technology, but only to a certain extent. Major corporations, small and large businesses, as well as private citizens, feel that not enough is being done to protect user privacy when it comes to things like devices, programs, and websites, to name a few. There are steps you can do to protect personal information, such as periodically updating your passwords and scanning the websites you visit for odd activity or links you should not click. Nevertheless, technology creates a catch-22 situation where you run the risk of having your privacy stolen. The same content can be hacked or tapped into by a knowledgeable person or group of people with bad intentions, just when you believe you have something to help secure you and your personal information.

b. **Given the development of technology, is it ever possible to maintain some sort of privacy whether using a computer, a cellphone, or even in your own home?**

The methods used to collect and store personal data are evolving along with technology. People are trying to figure out how to breach your personal space even when you think you have a solution to a

privacy-related issue. It often appears necessary to be one step ahead of the offender. To decide on the best course of action in an effort to increase personal privacy, you must think like one. Depending on the aspect of privacy you wish to secure, this is a separate task that may take more time to comprehend.

4.3.2 **Findings of Overall Results**

The following observations were drawn from the results of the questionnaires, the interview and focus group discussions held with subjects. Individuals of all ages and professions answered questions to gauge how unpleasant specific devices were to them in terms of privacy infringement.

The results reveal that the protection of one's personal space and right to privacy are important to people. People prize having some degree of control over who knows what about them. Of course, they do not want anyone to ever have access to their private information. Recent developments in information technology, however, put privacy at risk, lowered the degree of control over personal data, and increased the likelihood of a variety of unfavorable effects as a result of access to personal data.

What is the impact of technological advancements in developmental society?

Ancient and modern human civilizations both benefited and were hindered by technological innovations, inventions, and technical applications used in society to perform specific tasks. For societies to develop and prosper, technological innovations have become necessary, and at the same time, the culture, ideals, and aspirations of human society have shaped how these civilizations create, benefit and hindered by technology.

In the modern world, it is as simple as using Google search, podcasts, or YouTube videos to learn virtually any skill you need to succeed, whether it is a new language, programming language, engineering technical skill or confusing part. Of history. Instead of having to learn from print books, eBooks and even webinars now allow everyone to learn faster and more efficiently, while with the convenience of mobile computing systems or applications. motion. Online portals and websites also

enable educational institutions to deliver educational materials in a completely new, simplified way, helping students master the material using the computer systems they are familiar with. and also allows them to consolidate their teaching materials in one place.

What are socio-economic threats and privacy concerns caused by the adoption of new technology

One of the main ethical dilemmas in our technology age concerns how companies use personal information. As we browse websites, make purchases online, enter our information on websites, interact with various online businesses and engage in social media, we continuously provide personal information. Companies often collect information to hyper-personalize our online experience, but to what extent does that information really affect our privacy?

As the saying goes, personal information is the new gold. We have commoditized data for the value it brings to businesses trying to reach their customers. But when does it go too far? For businesses, knowing what types of products are searched for and what types of content people are viewing the most is extremely helpful. For politicians, it is important to know what types of social or legal issues get the most attention. These valuable data points are often leveraged for companies or organizations to make money or achieve their goals. Facebook in particular has been repeatedly criticized over the years for selling the personal data it collects on its platform.

What preventive measure can be put in place for the impacts of security and privacy intrusion

At a minimum, your privacy policy should include abuse detection and prevention procedures, as well as instructions for conducting internal investigations. It should identify the potential consequences of misuse. Start by reading your existing security policies, especially those related to incident management. Redo parts based on insider's trust. For example, your incident management plan shouldn't require your team to contact the administrator of a suspicious system to gain access to it; he or she could be the culprit.

Whether you own physical security or not, make it your number one priority. Just keeping people away from your critical infrastructure is enough to prevent most internal problems. Consider what

happened to Red Dot, a Seattle-area heating and air-conditioning company, where two janitors ransacked trash cans, desks, and file cabinets, stealing personal information. They obtained fraudulent credit cards and illegally accessed bank accounts, stealing tens of thousands of dollars before being caught.

The password is out of date. The password cracking technology is quite advanced, and stronger passwords create a forest of notes afterwards on the screen. And many employees share passwords. Alternatives are expensive and generic implementations are beyond the reach of most organizations. A more cost-effective compromise is to apply strong multi-factor authentication only to particularly sensitive applications or systems, such as HR or accounting. If you implement multi-factor authentication - combine user ID and password with token, smart card or fingerprint reader etc. - note that these methods may not fill all holes. Once your session is established, a knowledgeable insider can forge new transactions in your name or simply use your computer while you're away. Windows stations can be configured to lock users out after a fixed period of inactivity and require re-authentication.

4.3.3 **Summary**

Regrettably, modern technology has made it impossible to maintain your privacy, particularly online. Currently, every human being is the subject of data generated every day by millions of cameras, gadgets, and sensors. Also, a lot of people unwittingly give their information away by using the internet. Thus, despite our want to be private, it is difficult.

CHAPTER 5 SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 **Introduction**

This research is focusing on the impact of Security and privacy concern due to technology advancement. The background and the statement of the study have details showing what motivated the researcher to carry out the study. The objectives of the study were to assess the impacts of technology Advancements in developing societies, to analyze the socio-economic threats and privacy concerns caused by the adoption of new technology, to determine how impacts of security and privacy intrusion can be prevented and to examine how to enable trust for digital information and data transactions in such technology advancements. These objectives were highlighted in order to guide the researcher on research questions.

The research also covered literature review in line with impact of Security and privacy concern due to technology advancement. The literature review took a general approach to issues relating to the study. The research objectives were able to guide the researcher on the themes to cover on the review of the literature.

The study also covered the research methodology where it focused on the research design to be used. The target population for the study comprised of workers in electronics retail sector, technology end user, government employees in Harare Central Business District. Sample size was calculated using Taro Yamane's (2000) sample calculation formula. The researcher used self-administered questionnaires as the research instrument. Descriptive statistics and regression test were used to analyze data and results were presented in tables in percentages.

5.2 Discussion

Assess the impacts of technology Advancements in developing societies

Although technology has a significant impact on the gathering, storing, retrieval, and transmission of information, its main ethical ramifications concern the modification and accessibility of information. This opens up the option of wider access to information in addition to simultaneous access. More

people can now easily access a person's personal information as a result. Nonetheless, some security measures, like passwords, can prevent people from accessing necessary computer data. It should be mentioned that information processing technology advancements generate significant concerns about people's privacy. These problems mostly concern the availability and manipulation of information. Information specialists who deal with sensitive data should take particular note of this. The principles of liberty, truth, and human rights can be used to create workable standards for addressing these problems.

Impacts of security and privacy intrusion can be prevented

Large volumes of personal data may now be transferred and analyzed in mere seconds because of advancements in information technology, such big data and cloud computing. The information of billions of people is accessible on digital sites like Facebook or YouTube. They utilize strong algorithms to evaluate data in a number of ways, partially to customize the user experience. Yet, the use of AI by businesses to develop and use these algorithms presents some unethical concerns. The biggest problem is that these corporations don't disclose anything about their algorithms and AI. Regarding the sharing of personal information with other parties in particular, this lack of openness has significant privacy concerns. This intrusion can be prevented if these big companies are clear about their intentions and also if they have proper short documentation on their terms and conditions.

Examine how to enable trust for digital information and data transactions in such technology advancements

A number of recent technological developments have had, or may have in the future, a major impact on privacy and data protection. For instance, the rise of online services, e-commerce, the Internet of Things, and the application of technology-by-technology businesses' increasingly potent algorithms and artificial intelligence present difficulties that federal privacy regulations may not be able to address.

In a broad sense, the enormous progress in data processing capacity is the primary factor that information technology has had on privacy. Just think about how quickly information can now be processed—just type something into Google and, oftentimes, you'll see a variety of results that are in fact relevant to your search, even if you entered it incorrectly.

But, the use that some players decide to make of the technology, not the technology itself, is the issue. One of the most frequent instances is monitoring, which serves as the foundation for contemporary targeted advertising. Think about the time you searched for something on Amazon and then saw an Amazon advertisement for it while browsing a completely unrelated website. Ad targeting at its finest. Not only does Amazon keep track of your searches, but what happens when someone visits a website of a business and suddenly starts seeing advertisements for that business appear in unexpected places? Because all of our interconnected systems can talk with one another, this is possible, allowing information to follow you without your knowledge. This would require people to observe you walk around and record your actions as you work, which would not have been conceivable before the internet or on the current scale. This would be regarded as harassment and most likely be taken seriously. scared.

The business environment and IT both pose privacy issues. There is a chance that the business could see your e-mail even if you use your work computer to check it with permission from the corporation. You are deserving of it because you used your computer and network, and at worst, what you did on your personal email may result in your termination.

5.3 Conclusions

It all depends on how the craftsman uses the tool, which is technology. Additionally, technology has made some incredible advancements in privacy. When used properly, modern cryptography systems enable truly secure communications that cannot be intercepted by anyone, at least electronically, while the recipient reads your message and speaks to you over your shoulder to prevent someone from being in the room, but also prevent eavesdropping and eavesdropping attacks. When using the Internet, always employ encryption. As a result, providing your credit card information to make purchases on Amazon online is generally safe. The same technologies that have made it possible for some significant privacy violations also have the ability to impose greater levels of privacy than ever before.

Take a look at high-profile government examples where even powerful, enormous agencies were unable to "break into" properly implemented secure data repositories. We contend that while privacy should not be utilized to mask our behavior, it should still be regarded as a basic human right. We are all capable of exercising that right.

Therefore, it is nearly impossible to restore all the privacy that technology has stolen. "Sensors" are present everywhere since computers and communication chips are so compact. Your whereabouts could potentially be tracked by any technological gadget you carry. Your "smartphone" or tablet is simply a surveillance system with "side benefits" that is ready for business use. In a nutshell, it's a helpful diversionary tool. Due to technology innovation, the privacy issue has a dual aspect. Giving people their own space can help build great bonds and trust, but by doing so, they might end up hanging out with the wrong people, sharing inappropriate photos, and other things without your knowledge.

5.4 Recommendations

Data Protection

Big datasets produce outcomes that are more accurate and representative, but they also carry higher privacy threats. AI makes it simple to de-anonymize even seemingly anonymized personal data. Researchers discovered, in particular, that even coarse datasets had little anonymity and up to 95% re-identification. This indicates that there is a risk of being easily identifiable and data leakage without privacy measures. The use of AI for tax preparation and benefit eligibility analysis can likewise raise a concern.

Data Control

When AI learns to see patterns and characterize them, it will be able to make inferences and decisions that will improve or simplify your online experience. Yet, when AI produces inaccurate or unfavorable outcomes, it calls into question whether the judgments were made fairly. For instance, AI that is used

to evaluate credit risk may mistakenly lower credit limits for those who fit particular profiles. These choices could be made without your knowledge, consent, or even approval, particularly if the data used to make them was obtained without your consent.

The simple fact is that your private information might be used against you at times and without your knowledge. Fortunately, privacy concerns were handled by the developers throughout the pre-production development phase. In this way, we can keep benefiting from AI's technological advancements without compromising people's privacy. We advise integrating AI into your organization's data governance policy and committing resources to data protection, security, and AI supervision in addition to the development of AI products in order to increase data protection.

Consent and Control

Considering the element of the idea of privacy that we have thought about, people decide how and what information about themselves they wish to reveal to others in casual interpersonal encounters. You can actively participate in the process of character development by choosing the information you seek. This violates a number of normative prohibitions against individuals trying to collect specific kinds of information about other people without their agreement. There seems to be no equal possibility for control or consent with automated data gathering technologies. Automatic data gathering methods appear to exclusively consider their own conclusions while completely ignoring the goals of the data subjects.

5.5 Suggestions for Further Research

They are areas of interest that the researcher of this study has underlined for future research and would be very helpful if they could be further investigated. They consist of:

Location tracking

Your mobile phone automatically registers the position of base stations every few minutes when it is turned on. So, despite the fact that cell service providers keep track of their users' locations, the government can always access personal information without a court order. In addition, governments can gather data with the use of various location monitoring technology in order to identify or make

public significant enterprises that are connected to you. Where are you right now, where have you been, and all previous information.

Medical and Genetic Privacy

Health records should be kept secret since genetic and medical information can expose personal information. Hence, maintaining control over such information is crucial. Threats to autonomy and privacy are growing as medical records are digitized and DNA sequencing technology improves in price and speed.

Internet Privacy

With the use of modern technology that makes the procedure simpler, businesses and governments may now simply collect the specifics of their online behavior. Personal data can now be easily gathered by the business and sold to the highest bidder. At the same time, obsolete surveillance and privacy technologies enable governments to watch citizens in unprecedented ways.

APPENDIX 1 : AUREC APPROVAL LETTER

Investing in Africa's future

AFRICA UNIVERSITY RESEARCH ETHICS COMMITTEE (AUREC)

P.O. Box 1320 Mutare, Zimbabwe, Off Nyanga Road, Old Mutare-Tel (+263-20) 60075/60026/61611 Fax: (+263 20) 61785 website: www.africau.edu

Ref: AU2445/22 12 December, 2022

TATIANA NGAATENDWE NYANHONGO
C/O CBPLG
Africa University
Box 1320
MUTARE

RE: TECHNOLOGICAL ADVANCEMENT : A CAUSE FOR SECURITY AND PRIVACY CONCERNS

Thank you for the above titled proposal that you submitted to the Africa University Research Ethics Committee for review. Please be advised that AUREC has reviewed and approved your application to conduct the above research.

The approval is based on the following.

a) Research proposal

- **APPROVAL NUMBER** AUREC 2445/22
  This number should be used on all correspondences, consent forms, and appropriate documents.
- **AUREC MEETING DATE** NA
- **APPROVAL DATE** December 12, 2022
- **EXPIRATION DATE** December 11, 2023
- **TYPE OF MEETING** Expedited
  After the expiration date this research may only continue upon renewal. For purposes of renewal, a progress report on a standard AUREC form should be submitted a month before expiration date.
- **SERIOUS ADVERSE EVENTS** All serious problems having to do with subject safety must be reported to AUREC within 3 working days on standard AUREC form.
- **MODIFICATIONS** Prior AUREC approval is required before implementing any changes in the proposal (including changes in the consent documents)
- **TERMINATION OF STUDY** Upon termination of the study a report has to be submitted to AUREC.

Yours Faithfully

Miti G.P.
RESEARCH OFFICER: FOR CHAIRPERSON
AFRICA UNIVERSITY RESEARCH ETHICS COMMITTEE

APPENDICES:2

Security and Privacy Concern Questionnaire

Thank you for agreeing to participate in this survey. The purpose of this study is to investigate user awareness and concerns of online privacy and security and we ask for your help. The entire study should take at most 20 minutes.

You will not be compensated for your participation you can choose to participate in this

study voluntarily, and can quit at any time without submitting your survey answers, just close your browser window. You can also skip questions that you do not feel comfortable answering. If you have any question or concerns about this study, please contact the principal investigator…Nyanhongo Tatiana ...

If you have any question about your right as research participant, please contact Africa University research Compliance office at (020) 60075 or 60026 extension 1156 email aurec@africau.edu

This study is completely anonymous, your personal information is not collected and you can't

be identified from results of this study in anyway. By clicking Yes below, I acknowledge that I have read this consent form and I understand what is requested of me as a participant of this study. I freely consent to participate and certify that I am between 18 and 65 years old. To continue please click yes.

Do you want to continue? *

○ Yes ○ No

What is your age range?

○ 18-25

○ 26-34

○ 35-40

○ 40-65

○ Above 65

What is your gender?

- Male
- Female
- Other_____

What is your level of education?

- Primary
- Secondary
- Vocation / Polytechnic/University

In which country are you from? *

Zimbabwe

What is the language in which you are most fluent?

English

Do you use the Internet, at least occasionally? *

Yes No

Do you have a smartphone?

Yes No

What device do you mostly use to access the internet? *

Yes No

Are you familiar with the term privacy?

Yes No

We'd like to know if any of the following information about you is available on the Internet for others to see. It doesn't matter if you put it there yourself or someone else did so.

Your employer or a company you work for					
Your home phone number					

Your cell phone number					
Your date of birth					
A photo of you					
Your home address					
Things you've written that have your name on them					

How concerned are you about availability of your private information on the Internet?

- Not concerned
- Somewhat Concerned
- Very concerned

Are you concerned about these personal information being on the internet?

- Yes
- No

Are you familiar with web cookies?

- Yes
- No

How concerned are you about web cookies?

- Not conerned
- Somewhat Concerned
- Very concerned

Considering everything you know and have heard about the Internet, do you think it is possible for someone to use the Internet completely anonymously – so that none of their online activities can be easily traced back to them?

- Yes

INFORMED CONSENT GUIDE

My name is **Nyanhongo Ngaatendwe Tatiana**, a final year (Computer Information Systems) student from Africa University of Zimbabwe, I am carrying out a study on **Technological advancement: A cause for security and privacy concern** I am kindly asking you to participate in this study by answering the questions in a questionnaire.

Purpose of the study:

Thank you for agreeing to participate in this survey. The purpose of this study is to investigate user awareness and concerns of online privacy and security and we ask for your help. The entire study should take at most 20 minutes.

You will not be compensated for your participation you can choose to participate in this

study voluntarily, and can quit at any time without submitting your survey answers, just close your browser window. You can also skip questions that you do not feel comfortable answering. If you have any question or concerns about this study, please contact the principal investigator **Nyanhongo Ngaatendwe Tatiana**

If you have any question about your right as research participant, please contact Africa University of Zimbabwe research Compliance office at telephone (020) 60075 or 60026 extension 1156 email aurec@africau.edu

This study is completely anonymous, your personal information is not collected and you can't

be identified from results of this study in anyway. By clicking Yes below, I acknowledge that I have read this consent form and I understand what is requested of me as a participant of this study. I freely consent to participate and certify that I am between 18 and 65 years old.

Offer to answer questions

Before you sign this form, please ask any questions on any aspect of this study that is unclear to you. You may take as much time as necessary to think it over.

Authorisation

If you have decided to participate in this study, please sign this form in the space provide below as an indication that you have read and understood the information provided above and have agreed to participate.

---------- ----------

Name of Research Participant (please print) Date

---------- Signature of Research Participant or legally authorised representative

If you have any questions concerning this study or consent form beyond those answered by the researcher including questions about the research, your rights as a research participant, or if you feel that you have been treated unfairly and would like to talk to someone other than the researcher, please feel free to contact the Africa University Research Ethics Committee on telephone (020) 60075 or 60026 extension 1156 email aurec@africau.edu

Name of Researcher **Nyanhongo Ngaatendwe Tatiana**

Reference

How Society and Technology Become Partners in Changing Our Lives By DJ Wardynski | Published October 24, 2019

Ways to prevent computer security threats from insiders David Bianco, May 2019

Antecedents of Trust and Adoption Intention toward Artificially Intelligent Recommendation Systems in Travel Planning: A Heuristic–Systematic Model Si Shi, Yuhuang Gong, and Dogan Gursoy 2020

Positive & Negative Impact of Technology on Society . Edelman's Trust Barometer 2020,

Positive impact of technology on society. 26 November 2021 Patrycja Paterska