Analyzing the Impact of Ethical Issues in E-Government Implementation: A Case of Zambia

By

EDDIE LIYWALII

A dissertation submitted to the University of Zambia in partial fulfilment of the requirements of the Degree of Master of Engineering degree in Information and Communication Technology Policy, Regulation and Management

University of Zambia

Lusaka

2019

Dedication

This document is dedicated to my wife, Abby, and our three sons Sean, Hans and John who supported me throughout my studies.

Copyright Declaration

I, Eddie Liywalii, do hereby declare that the content of this document is my own and all other works by other people have been duly referenced, and that this work has not been previously presented to another university for the same purpose.

…….. ……

Eddie Liywalii Date

Certificate of Approval

This dissertation of Eddie Liywalii has been approved as fulfilling the requirement for the award of Master of Engineering in ICT Policy, Regulation and Management by the University of Zambia.

Name: ……..

Signature: ……

Date: ……...

Name: ……..

Signature: ……

Date: ……...

Name: ……..

Signature: ……

Date: ……...

Name: ……..

Signature: ……

Date: ……...

Acknowledgements

Foremost, I would like to acknowledge the Almighty God, for keeping me in good health throughout the rigors and demanding tasks of the research study, and for keeping my mind focused during the long hours, days and nights, spent on searching and researching. My sincere heartfelt gratitude goes to Dr. Simon Tembo for the fatherly guidance and encouragement he gave me during the process of working on this research. The work appeared near impossible in my imagination, but through his valuable support and guidance I managed to deliver expected outcomes.

Finally, I would like to express my very profound gratitude to my beloved wife and 3 lovely sons, my parents, and brothers and sisters for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

Abstract

E-government is intended to enhance the access to and delivery of government services to benefit citizens, business partners and employees while reducing corruption and costs but increasing transparency and revenue growth on the other hand.

Despite the foregoing, the use of ICTs in both public and private sector, at individual and institutional levels, has brought about a spectrum of ethical challenges in our societies thereby undermining efforts made to encourage citizens adopt the use of electronic services deployed for public service. The objectives of this research were to establish what ethical issues arise in e-government implementation especially in developing countries, in this case Zambia and the impact these ethical issues have on e-government implementation. In addition, to understand how IT systems can be designed to address the identified ethical issues that arise in e-government.

From the research, it was established that the prominent ethical issues that arise in e-government implementation are security and privacy. 44% of the respondents agree, in addition to 28% who strongly agree, that the inclusion of ethical issues in planning of e-government will contribute to the successful implementation of e-government. Only 38.5% of the respondents affirm that the current e-government policy addresses these ethical issues in e-government implementation while 30.8% disagree and another 30.8% are not sure.

This study recommends that a holistic approach to the addressing of these ethical issues should be adopted by governments to avoid formulation of policies in silos. The design of such policies must precede any systems design as systems design must manifest efforts to address the ethical issues that arise in the use of the particular systems concerned using Value Sensitive Design.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AI	Artificial Intelligence
ECT	Electronic Communications and Transactions
EIZ	Engineering Institution of Zambia
G2C	Government – to – Citizens
G2E	Government – to – Employees
GDPR	General Data Protection and Regulation
HTML	Hyper Text Markup Language
ICT	Information and Communications Technology
ICTAZ	Information and Communications Technology Association of Zambia
IT	Information Technology
ITU	International Telecommunications Union
NDP	National Development Plan
NISP	National ICT Strategic Plan
PDE	Policy Design Effect
RPT	Resource Product Target
UAS	Universal Access and Service
UNESCO	United Nations Educational, Scientific and Cultural Organization
VSD	Value Sensitive Design
ZABS	Zambia Bureau of Standards
ZAMCOPS	Zambian Music Copyright Protection Society
ZICTA	Zambia Information and Communications Technology Authority

CHAPTER 1

1.0 Introduction

E-government refers to the use by government agencies of information and communications technologies ICTs (such as Wide Area Networks, the Internet, World Wide Web (WWW) and mobile computing) that have the ability to transform relations with citizens, businesses, and other arms of government. These technologies can serve a variety of different ends: better delivery of government services to citizens, improved interactions with business and industry, citizen empowerment through access to information, or more efficient government management. The resulting benefits can be less corruption, increased transparency, greater convenience, revenue growth, and/or cost reductions. (Palvia and Sharma, 2007) E-government is intended to enhance the access to and delivery of government services to benefit citizens, business partners and employees.

Despite the foregoing, the use of ICTs in both the public and private sector, at individual and institutional levels, has brought about a spectrum of ethical challenges in our societies. This is the case for both developed and developing countries. According to Quinn (2014), **Ethics** is the philosophical study of morality. It is a rational examination into people's moral beliefs and behavior.The word **morality or morals** on the other hand describes standards or codes of behavior expected of an individual by a group (nation, organization, profession) to which an individual belongs in their pursuit of shared 'core **values**' – such as life, health, happiness, security, resources, opportunities and knowledge – which are so important to the continued survival of communities. The analogy in figure 1.1 by Quinn (2014) gives an illustration of the difference between ethics and morals;

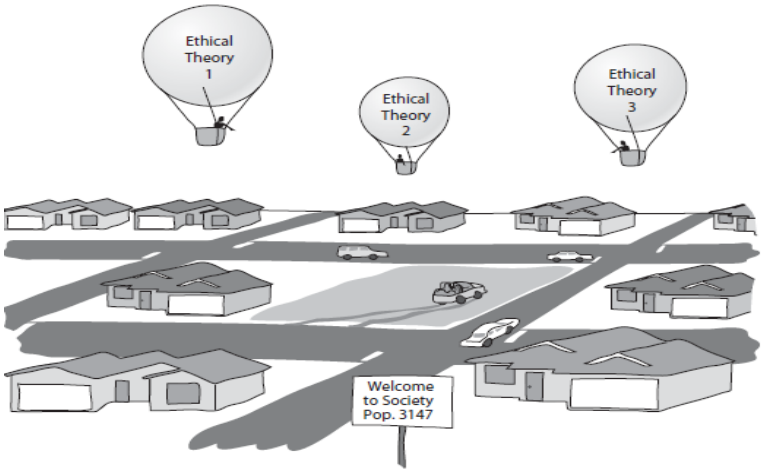

Fig 1.1: An analogy explaining the difference between ethics and morality. Imagine society as a town. Morality is the road network within the town. People doing ethics are in balloons floating above the town [*Quinn (2014)*]

An ethical issue is a problem or situation that requires a person or organization to choose between alternatives that must be evaluated as right or wrong. (Business dictionary)

A thorough understanding of the ethical issues that arise as a result of the adoption and deployment of ICTs for better delivery of public services will greatly help developing countries to employ strategies that will increase chances of successful implementation of e-government against a backdrop of limited resources and high failure rate of information technology projects. (Levinson, 2006)

As already alluded to earlier, in most cases, in Africa and Zambia in particular, the mention and use of ICTs always raises concerns of data security and privacy among other issues. However, the mention of these terms and where they are discussed in many academic literature and policy documents, they are not comprehensively and extensively tackled from an ethical point of view. For instance, one of the main, and among the first documents outlining government's efforts to implement e-government in Zambia is the National ICT Policy of 2006, only notes security in the information society as a mere 'concern' but not an ethical or moral issue. Already, therein

lies the problem; since security and any other ethical issues for that matter, are not recognized as an ethical issue, it also follows that the framework upon which solutions will be developed to address these concerns will ultimately not yield satisfactory results to the problem then.

Similarly elsewhere, in South Africa for instance Manda and Backhouse (2016) in their paper, outline the need to addressing trust, security and privacy 'concerns' in e-government integration, interoperability and information sharing through policy. Here too these are 'concerns' without mention of the term ethical issues. Farelo and Morris (2006) look at the Status of e-government in South Africa and identify legal frameworks, governance models, infrastructure and human resource development as key success factors. Implicitly, ethical issues are none key factor.

In Rwanda, Twizeyimana et al (2018) study found six overarching categories of aspects that challenge a successful implementation of e-government, they include information infrastructure for e-government, social inclusion, governance, management, trust in the new system, and languages. Ethical issues are not part of their findings.

This research tries to explore the new knowledge about ethical issues and their impact on e-government. This is more critical especially in the wake of artificial intelligence; where advanced information systems called expert systems are becoming commonplace in the provision of public services in areas such as medical diagnostics, unmanned aircrafts, and driverless taxis, to mention inter alia.

1.1 Background

E-governance and e-government are terms treated to be similar; however, there are some differences between the two. There exists various definitions from different perspectives by different scholars for these concepts. According to Sharma (2014), e-government is the use of the

ICTs in public administrations combined with organizational change and new skills to improve public services and democratic processes and to strengthen support to public policies.

Table1.1 E-government and E-governance [*Singh (2017)*]

E-Government and E-Governance	
Government	**Governance**
Superstructure	Functionality
Decisions	Processes
Rules	Goals
Roles	Performance
Implementation	Coordination
Outputs	Outcomes
E-Government	**E-Governance**
Electronic service delivery	Electronic consultation
Electronic workflow	Electronic controllership
Electronic voting	Electronic engagement
Electronic productivity	Networked societal guidance

Apart from being a means to an end, ICTs require governance themselves too. A substantial growth in regulation and policy making capacities, with all the capability and opinion making processes, among the different social stakeholders of these matters is essential. Hence, the perspective or definition of e-governance on the other hand is "the use of the technologies that both help governing and have to be governed". (Sharma, 2014) The introduction of ICTs in government for governance in a process referred to as the adoption and deployment of e-government, or e-government implementation, has come along with many implications. Among other things are ethical issues, some of which if not all, may not be new but another dimension or more added to them. Singh (2017) gives a summary of the differences in activities of government and governance contrasting this with e-government and e-governance in Table 1.1 above.

Our modern society is called “the information society”. This is because of the pivotal role that is played by intellectual, intangible assets in form of information, computer software and hardware,

in information-intensive services (business and property services, communications, finance, and insurance), and in public sectors (education, public administration, health care). This has culminated into what is now called knowledge-based economies.

As a social organization and way of life, the information society has been made possible by a cluster of ICT infrastructures which are a full expression or manifestation of a knowledge area called techne. (Himma 2008)

On the other side, the information society has already posed fundamental ethical problems, whose complexity and global dimensions are rapidly growing and evolving. Nowadays, a pressing task is to formulate an applied set of ethics (information ethics) that can treat the world of data, information, and knowledge, with their relevant life cycles (which include the creation, elaboration, distribution, communication, storage, protection, usage, and possible destruction), as a new environment called the infosphere, in which humanity is and will be flourishing. Information ethics should be able to address and solve the ethical challenges arising in this infosphere. This area of knowledge that deals with ethics is called phronesis. (Lee, 2010) In science and engineering fields the techne is always more emphasized than the phronesis. However, from the time Moore coined the word 'computer ethics' the study of ethics has been an area of interest to computer scientists. (Kizza, 2007)

Zambia, like other developing countries, in its quest to improve public service and efficiency in national resources management has also embarked on e-government implementation. Its efforts date back to early 2000 when the first National ICT Policy was developed. In 2016, a master plan called the SMART Zambia – e-Government Master plan (SMART Zambia, 2016), was released. In this document, it is noted that; The Government of the Republic of Zambia (GRZ) intends to transform the way it interacts and delivers services to citizens, businesses and across

government departments and agencies by bringing government closer to the people and making service delivery more friendly, convenient, transparent, efficient and cost effective through the implementation of e-Government. The services to be delivered electronically will be both informational and transactional. User groups of e-Government will include citizenry, businesses, and government departments themselves. The question that arises is, how is Zambia tackling the techne (infrastructure) as well as the phronesis (ethics) areas in the e-government project to ensure successful implementation?

1.2 Statement of the problem

There is a lack of well understood and developed rules and models for ethical behaviour in e-government and it is becoming evident that the same problems which beset e-business have also been thought to beset e-government, that is, a lack of well understood rules, trust and digital divide among others. (Horner and Mullen, 2004)

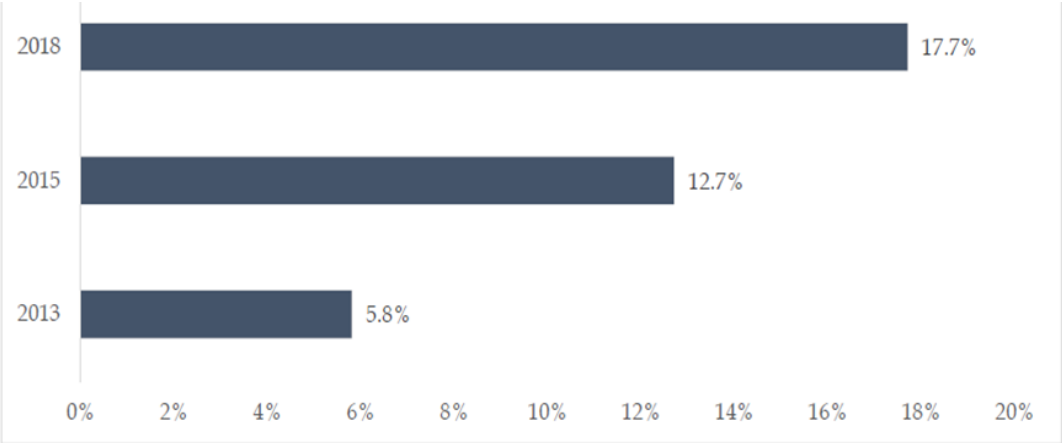

Fig 1.2: Access to Internet Services by Households; 2013- 2018 [*ZICTA (2018)*]

The above graph shows the levels of access to Internet services by households as reported in the National Survey on Access and Usage of ICTs by Households and Individuals Report by ZICTA.

In 2018, the access only stood at 17.7% only of the total population. In addition, the adoption of e-commerce by users of Internet services only stood at a dismal 8.9% national wide as shown below. (ZICTA, 2018)

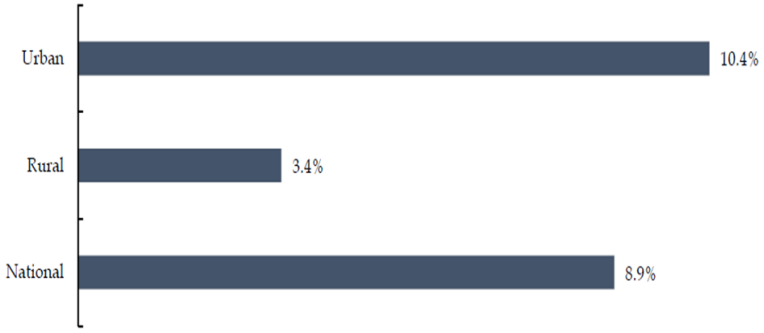

Fig 1.3: Adoption of e-commerce by users of Internet services across regions [*ZICTA (2018)*]

However, these appalling and discouraging figures are against the staggering figures of levels of awareness of the dangers of risks the users are exposed to in the use of Internet services as depicted in Figure 1.4 below.

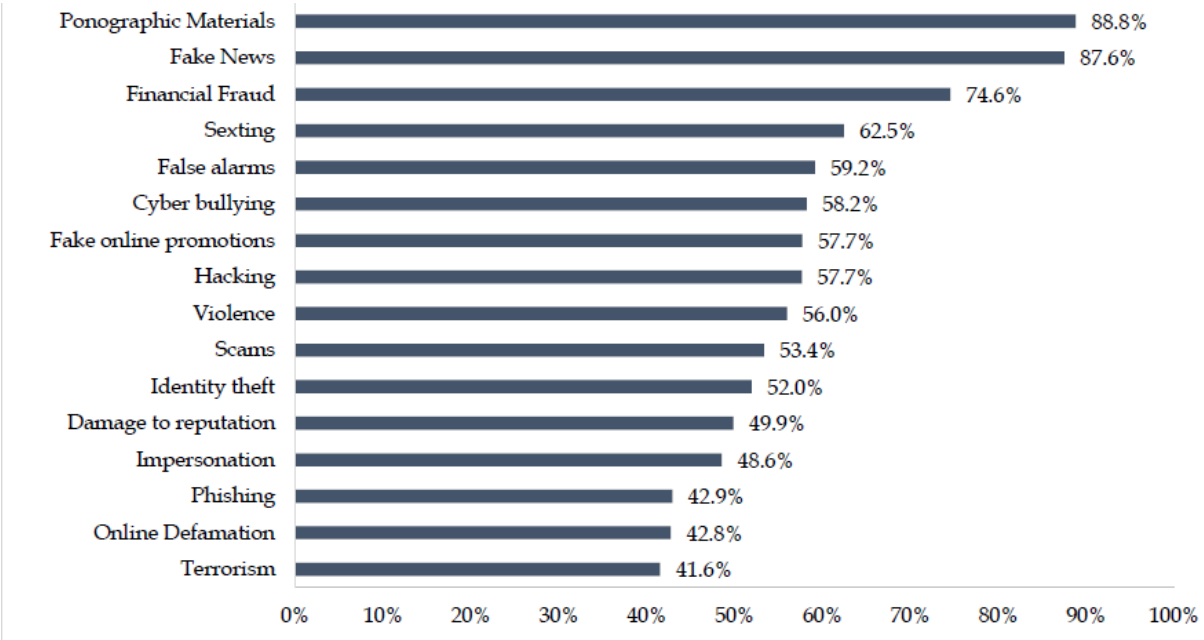

Fig 1.4: Levels of awareness of different types of dangers of the Internet risks [*ZICTA (2018)*]

The report does not indicate in any way at all if there is any correlation between the high levels of awareness of dangers and the low levels of Internet access and let alone the adoption of e-commerce by users of Internet services. This creates a knowledge gap and therefore necessitates a study to establish if the high levels of awareness of the Internet risks affects the adoption of e-commerce, let alone e-government in Zambia. The awareness of the above dangers can also be treated as ethical concerns (of ethical issues) by the users.

The literature reviewed classifies trust, digital divide and security as examples of some ethical issues that arise in the adoption and deployment of e-government. The other ethical issues are privacy, confidentiality, computer crime (cybercrime), computer decisions, technological dependence, reliability, integrity, (cyber) security, intellectual property, anonymity, legitimacy, internet addiction, computer technology for persons with disability. A holistic approach to establish and address all ethical issues that arise in e-government implementation is necessary for e-government success. It will also help understand if there are any generic similarities as well as interrelationships of any kind among these ethical issues. The holistic approach will also help tackle the problem of developing policies in silos. For instance, at national level, while developing policies to address cyber security, certain aspects of the security measures may undermine the privacy rights of citizens.

The above mentioned ethical issues affect both the G2C and G2E sides, meaning that they arise in two instances, when citizens access or would want to access the e-government services and when the implementers develop these systems and interact with the e-government services to provide services to the consumers respectively.

The problem identified is, do the implementers of e-government possess enough knowledge about all the ethical issues that arise in e-government adoption and deployment on the two sides

identified above? Is there enough knowledge about these ethical issues and their generic traits from both the academia and practitioners of e-government? What impact do these ethical issues have on e-government and what measures can developing countries make to address the impact? These concerns regarding the discrepancy in the body of knowledge and industry needs in ethical issues arising in e-government deployment necessitate a study to establish how;

a. The inadequate knowledge of all e-government ethical issues among IT scholars and IT policy practitioners in e-government impacts e-government adoption and deployment
b. The absence of policy frameworks for the resolution of these ethical issues affects the implementation of e-government through development of systems that adequately address the arising ethical issues
c. These ethical issues come to the fore in the wake of artificial intelligence (AI) where autonomous agents called expert systems, in some instances with algorithms enabling machine learning, are now deployed to offer public services as part of e-government
d. The absence of an IT professional ethical regulatory framework affects public perception, security and privacy to create public confidence in the use of information systems for e-government.

The national ICT policy talks about human and intellectual capital as the most important resource of any given country in the quest for sustainable social and economic development. It is also acknowledged in the policy that the extent to which Zambia will benefit from the advances and the opportunities of the emerging information society will largely depend on the country's capacity to develop and harness the available human resource to support national development. (National ICT Policy, 2006) In a way this includes how much human and intellectual capital is

available in the phronesis knowledge area just as in the techne knowledge area of ICT deployment for successful e-government implementation.

1.3 Aim or Purpose of the study

The aim of this study was to establish how ethical issues that arise in the two e-government interactions, G2E and G2C affect e-government implementation and recommend how systems could be designed to address the identified ethical issues.

The study of ethics has been an area of interest to computer scientists since Moore coined the word "computer ethics". According to James H. Moore, who is believed to have first coined the phrase "computer ethics," computer ethics is the analysis of the nature and social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of such technology. (Kizza, 2007) This definition justifies the study of ethics and policy by computer scientists to understand the impact of computer technology on users and how to design systems that address them.

The study brought to the fore the often overlooked deficiencies in the human capacity, in terms of awareness of the impact that ethical issues have on e-government, with respect to policy makers and e-government practitioners (G2E) in the development of information systems, rather than the often generalized view of citizens' illiteracy levels (G2C) in the e-government implementation and the need for study in this area with respect to developing countries, in this case, Zambia.

The study focused on ethical issues that arise in e-government implementation in the two e-government interactions G2C and G2E.

1.4 Study Objectives

1. To establish what ethical issues arise in e-government and analyze the bearing these ethical issues have on e-government adoption and deployment
2. To review the policies and mechanisms that could address these ethical issues for successful implementation of e-government
3. To understand how to design systems that address the identified ethical issues in e-government implementation especially in the introduction of artificial intelligence (AI)
4. To establish the role that IT professional ethics plays on e-government implementation

1.5 Research questions

1. What are the ethical issues that arise in and how do these ethical issues impact the implementation of e-government?
2. How do policy makers and analysts resolve these ethical issues for successful implementation of e-government?
3. How should systems be developed to ensure successful implementation of e-government against these ethical issues in the wake of artificial intelligence (AI)?
4. How does the establishment of a professional regulatory framework help to successfully implement e-government?

1.6 Significance of the study

In line with the above objectives, the significance and contribution of the study are as follows;

1. The study introduces a new approach to system design which; is identification of all ethical issues that arise in e-government implementation from the ethical perspective

2. The study introduces a framework that can be used to isolate ethical issues that arise on the G2C and G2E interactions of e-government
3. The study also establishes that the identification of these ethical issues and formulation of the policies to address them preceded any system design and implementation.

The significance of this study is emphasized in Moore's observation that there are times when policy vacuums are created in the decision-making processes, especially those that involve processes in which computer technology is "essentially involved". (Kizza, 2007) Quinn (2014) also notes that the study of ethics is particularly important right now. Our society is changing rapidly as it incorporates the latest advances in information technology, and is now called an electronic society (e-society). Just think about how cell phones, portable digital music players, tablets, and social media apps have transformed how we spend our time and interact with one another! These inventions have brought us many benefits. However, in the same breath, some people selfishly exploit new technologies for personal gain even; that reduces the overall benefit of these technologies for the rest of us. Here are two examples. While most of us are happy to have the ability to send email to people all over the world, others engage in "phishing" to steal financial information. Access to the World Wide Web provides libraries with an important new information resource for their patrons, but should children be allowed to follow links leading to pornographic Web sites? This raises the question of ethical issues in our modern society today and policies need to be designed for successful implementation of e-government.

On the other facet, the emergence of artificial intelligence (AI), has brought to the fore another dimension of ethical concerns in the now ubiquitous deployment of autonomous computer systems called expert systems to perform duties initially performed by humans and provide a service to the public especially in developed countries.

Due to globalization, developing countries, including Zambia, could start bracing themselves for this new norm in the new era of information age. New phenomena such as virtual reality (VR), an environment that simulates the reality of "other worlds" through modeling and creating better tools for understanding the complexities of our world and the cyberspace (CP), an environment that investigates the reality of the assumed presence of objects and peers are all exciting technological frontiers offering novel environments with unlimited possibilities. (Kizza 2007) These have all pushed the existing frameworks of acceptable ethics to the limits while testing their ability to accommodate the new norms in our society without reaching their yield point.

1.7 Scope of the study

This study is limited to ethical issues that arise in the implementation of e-government (in G2C and G2E interactions) in developing countries, that is adoption and deployment of ICTs, in this case Zambia in particular. The study did not look at ethical theories and models for ethical decision making. It also did not look at the classification of ethical issues by how they arise in e-government nor the classification of ethical issues in association with applied ethics.

1.8 Theoretical Framework

There are so many conceptual and theoretical frameworks that have been developed in the study of e-government; its adoption, deployment and issues that arise in the process. Among the issues that arise in the implementation of e-government especially in developing countries are such issues as financial challenges to fund successful implementation of e-government projects, organizational restructuring, public policy issues, citizen participation, radical implementation of e-government that tackles or encompasses e-democracy and ethical issues. (Stahl, 2005)

Ethical problems are some of the major issues that seem to beset the successful implementation of e-government not only in developing countries but developed countries as well.

This research was meant to understand the effects that these ethical issues that arise in the implementation of e-government have in developing countries; in this case study of Zambia. In this vein, a theoretical framework for the study was developed as shown in a matrix (Fig 1.6) on page 14; this theoretical framework is an expansion of the two of the four interactions of e-government (Fig 1.5) as used by Pandey (2015) adopted from an E-Governance conceptual framework.

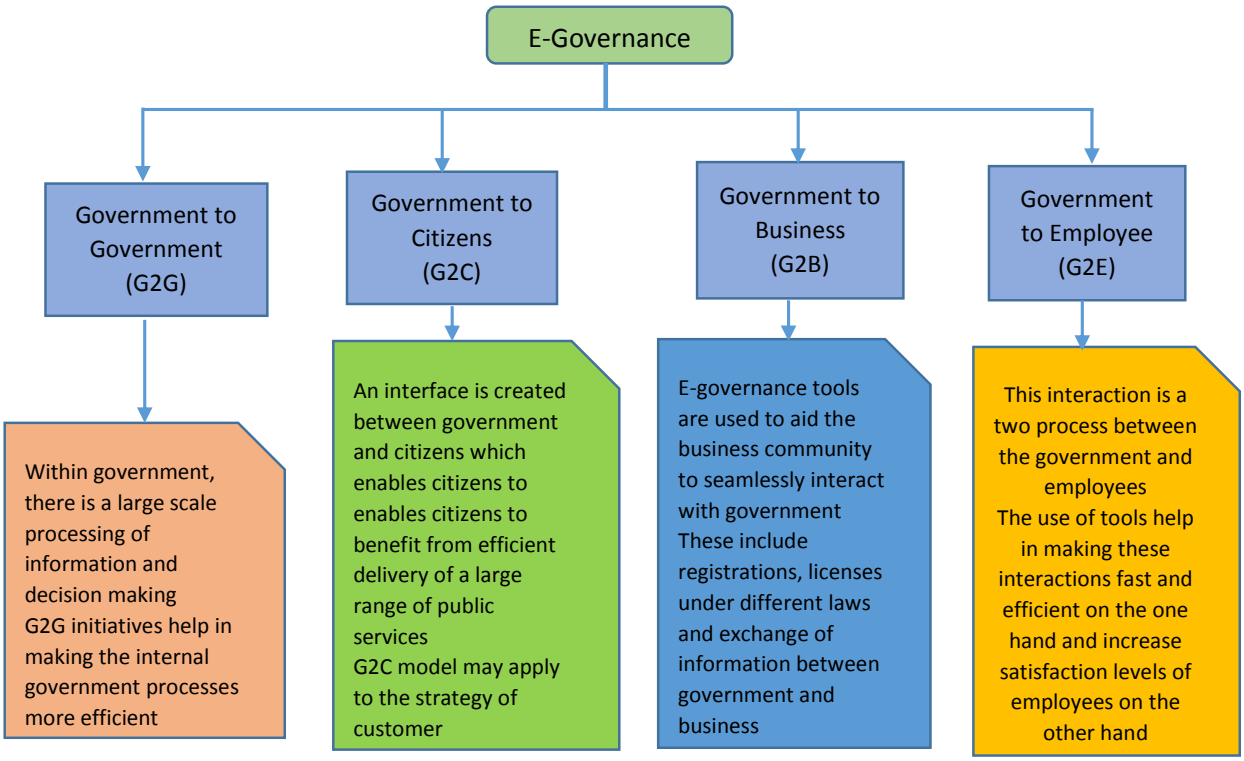

Fig 1.5: E-government interactions [*Pandey (2005)*]

The following weaknesses were observed with the existing system (e-government interactions):

1. Regards human beings as entities similar to institutions in the interaction with e-government services
2. Institutions are NOT moral beings

3. Humans are still behind the other two interactions (G2G) and (G2B) even where such interactions are automated

Table 1.2: The G2C/G2E Matrix [*Liywalii & Tembo (2019)*]

	Systems (Processes/Services)	**Humans**	
Internal	Ethical Issues to do with governance and democratic dispensation (G2E)	Ethical issues to do with professionals (G2E)	E-GOVERNANCE
External	Ethical issues to do with systems (IS) (G2C)	Ethical issues to do with users (G2C)	
E-SOCIETY			

This research sought to understand whether the ethical issues that arise in e-government implementation could be identified and categorized in the above manner. The possibility of classifying the ethical issues in the this way could lead to a better understanding of the definition of each category of ethical issues and their unique characteristics while providing a focused research for possible solutions to these uniquely identified categories of ethical issues arising in e-government implementation. All the four being interacting forces in an e-society where a system of governance employs ICT tools in its administration and delivery of services to the public. Therefore, Figure 1.6 is the proposed theoretical framework for this study.

1.9 Operational definitions

In this research, the conceptual definitions of the following terms are adopted as the operational definitions for the purposes of the study as follows;

E-government: refers to the use by government agencies of information and communications technologies ICTs (such as Wide Area Networks, the Internet, and mobile computing) that have the ability to transform relations with citizens, businesses, and other arms of government.

E-governance: is the use of the technologies that both help governing and have to be governed. On the other hand, e-governance focuses on public's participation and their role as citizens. (Kapucu, 2007)

Ethics: is the philosophical study of morality. It is a rational examination into people's moral beliefs and behavior.

Ethics of e-government: refers to the ethics that arise in the adoption and deployment of information and communications technologies in processes of governance, government administration and public service delivery. These ethics are said to be applied ethics as they belong to a branch of ethics which consists of the analysis of specific, controversial moral issues in a particular field, in this case, the field of computer science. The three main applied ethics that belong to e-government are computer ethics, information ethics and cyber ethics. (Ramadhan et al, 2011)

E-society: is a type of a society where an extensive use of and dependability on ICTs is present in achieving common interests and goals of major social stakeholders (citizens, businesses, government and public administration). This is also sometimes referred to as an information society.

Artificial Intelligence: is a field of study in computer science that endeavors to build computer systems with capabilities of emulating human knowledge.

Expert Systems: these are systems emanating from artificial intelligence built to mimic human experts in a particular field to provide a service.

Machine learning: is a method of data analysis that automates analytical model building. It is a branch of artificial intelligence based on the idea that systems can learn from data, identify patterns and make decisions with minimal human intervention. It is commonly used in data mining algorithms

Internal e-government ethics: these are e-government ethics that arise in the internal processes of policy formulation, planning and deployment of e-government by policy makers, analysts and government employees

External e-government ethics: these are e-government ethics that arise in the external processes of accessing e-government services by citizens

Values: pertaining to ethics, values are beliefs about what is right and wrong and what is important in life. The most widely shared core values are as life, health, happiness, security, resources, opportunities and knowledge.

Embedded values: these are values that arise in ethical questions asked during the designing and building of computer systems before use, such as; could there be an ethics of computer systems separate from the ethics of using computer systems? It aims to develop a theory and methodology for moral reflection on computer systems themselves, independently of particular ways of using them. The embedded values approach holds that computer systems and software are not morally neutral and that it is possible to identify tendencies in them to promote or demote particular moral values and norms. It holds, for example, that computer programs can be

supportive of privacy, freedom of information, or property rights or, instead, to go against the realization of these values.

Value-sensitive design (VSD): an approach to design developed by computer scientist Batya Friedman and her associates, which incorporates notions of the embedded values approach. The VSD approach is not an approach within ethics but within computer science, specifically within information systems design and software engineering. It aims to account for values in a comprehensive manner in the design process, and makes use of insights of the embedded values approach for this purpose. (Floridi, 2010)

1.10 Organization of Thesis

This thesis has been organized into five major parts called chapters. Chapter One which is the introduction discusses the problem background, problem statement, research questions, study objectives, scope and significance of the study. Chapter two goes on to review the literature from books, journals, articles and web sites that have published articles on the subject matter. Chapter three looks at methodology while chapter four discusses results obtained. Chapter five presents the conclusions and the recommendations that have been drawn from the entire study.

1.11 Chapter summary

Ethics is the philosophical study of morality. It is a rational examination into people's moral beliefs and behavior. The use of ICTs in both the public and private sector, at individual and institutional levels, has brought about a spectrum of ethical challenges in our societies.

A thorough understanding of the ethical issues that arise as a result of the adoption and deployment of ICTs for better delivery of public services will greatly help developing countries to employ strategies that will increase chances of successful implementation of e-government

against a backdrop of limited resources and high failure rate of information technology projects. This study seeks to understand the impact that these ethical issues have on the implementation of e-government in the case of Zambia based on the four-tie system in the IT industry identified in the National ICT Policy 2006.

CHAPTER 2

2.0 Literature Review

According to the UNESCO e-government toolkit for developing countries, the entire gamut of E-government involves a large number of entities and processes; however, there are primarily four types of interaction which form the foundation of e-government deployment:

a. Government to Government (G2G): interaction among government departments and agencies as they work to provide services to the public
b. Government to Citizen (G2C): interaction between government and citizens as they (citizens) want to access public services from their government
c. Government to Business (G2B): interaction between government and businesses as they (businesses) work to create wealth
d. Government to Employee (G2E): internal activities of government employees as they (employees) perform their duties. (UNESCO, 2005)

The above interactions are very vital and require equal attention in ensuring successful implementation of e-government. These interactions are depicted in figure 2.1 below;

Fig 2.1: E-government interactions [*UNESCO (2005)*]

The ITU e-government implementation tool kit on the other hand specifies an e-government environment with four basic dimensions: (1) infrastructure, (2) policy, (3) governance and (4) outreach. (ITU, 2009)

While this is not an exhaustive list of dimensions of e-government, these categories are considered to be wide enough to cover all the important aspects of e-government and can, at the same time, be narrowed down to provide useful recommendations on future policy prioritization and activities.

In this model, the IT professionals (working either as government employees and/or contractors) responsible for the deployment of ICT infrastructure fall under the governance dimension and are referred to as the IT back office for e-government. While the citizens and businesses accessing the public services are in the outreach dimension. Infrastructure is probably the most obvious and tangible dimension of e-government. This infrastructure for e-government provision is not linked to a specific technology, but rather to any electronic means that citizens and businesses use to send and receive voice, data, and images via the Internet, such as personal computers, laptops, personal digital assistant devices (PDAs), as well as mobile and fixed line telephony.

The other dimension is called the policy dimension. This dimension comprises the formulators of policies that influence the implementation of e-government. These policies include but are not limited to, for instance, the antitrust regulations and market liberalization strategies, enforced by telecommunication regulatory authorities, telecommunications marketing and competition laws, consumer protection, universal access and service to promote access to ICT infrastructure in least served areas, such as rural and low income communities. The above is summarized in figure 2.2 below;

Table 2.1: E-government dimensions [*ITU (2009)*]

Dimensions of E-Government	**Toolkit Modules**	
Outreach	Framework: Readiness assessment and action priorities	E-government services to citizens
		E-government services to business
		Interagency e-government services
Governance		IT Back office of e-government
		Re-engineering public processes
Policy		Laws on e-government security
		Institutional models of e-government
Infrastructure		Mobile infrastructure
		Broadband infrastructure

According to Moore, (believed to have first coined the phrase "computer ethics") computer ethics is the analysis of the nature and social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of such technology. (Kizza, 2007) Very few studies have been done on ethical issues that arise in e-government implementation and their (ethical issues) policy implications particularly in developing countries. Most of the studies have been done by information science and IT experts in Telecommunications and Computer Science fields. However, there still exists a knowledge gap on the ethical issues and how they impact the implementation of e-government, in particular the developing countries.

2.1 The ethical dimension of information systems

The introduction of information technology in our society has a ripple effect, raising new ethical, social, and political issues that must be dealt with on the individual, social, and political levels respectively. These issues have five moral dimensions. According to Laudon (2008) the major ethical, social, and political issues raised by information systems, in that order, include the following moral dimensions:

1) Information rights and obligations – this dimension refers to the question of what information rights individuals and organizations possess with respect to themselves and what they can protect.
2) Property rights and obligations – this refers to how traditional intellectual property rights will be protected in a digital society in which tracing and accounting for ownership are difficult and ignoring such property rights is so easy.
3) Accountability and control – refers to who can and will be held accountable and liable for the harm done to individual and collective information and property rights.
4) System quality – refers to what standards of data and system quality should we demand to protect individual rights and the safety of society.
5) Quality of life – here the question asked is, what values should be preserved in an information- and knowledge-based society? Which institutions should we protect from violation? Which cultural values and practices are supported by the new information technology?

These issues are first evaluated at an individual level as ethical issues before they become a social concern at a community level, eventually attracting the political leaders' attention owing

to society outcry thereby becoming political issues resulting in formulation of new laws and policies to tackle the concerns.

A look at some of the terms commonly used in the study of morals and ethics including definition of the terms law and rules for adherence to the agreed morals society as understood in the context of this study is given below;

2.1.1 Morality and Ethics

While Laudon (2008) defines ethics as the principles of right and wrong that individuals, acting as free moral agents, use to make choices to guide their behaviours. Quinn (2014) however, gives his definition of ethics as the philosophical study of morality or a rational examination into people's moral beliefs and behaviour. Quinn (2014) also defines morality as rules of conduct describing what people ought and ought not to do in various situations in a particular society. The word morality derives from moral which means according to Oxford dictionary principles of right or wrong behaviour. The word morals and morality are sometimes used interchangeably. Notwithstanding, according to Kizza (2007) morality concerns itself with a set of shared rules, principles, and duties, independent from religion, applicable to all in a group or society, and having no reference to the will or power of any one individual whatever his or her status in that group or society.

According to MacDonnell in Kizza (2007), moral theories "seek to introduce a degree of rationality and rigor into our moral deliberations". They give our deliberations plausibility and help us to better understand those values and the contradictions therein. Like the morals and ethics, moral theories are sometimes called ethical theories.

2.1.2 Values and Norms

The Internet Encyclopedia of Philosophy defines moral codes as rules or norms within a group for what is proper behaviour for the members of that group. The norm itself is a rule, standard, or measure for us to compare something else whose qualities we doubt. In a way, moral codes are shared behavioural patterns of a group. These patterns have been with us since the beginnings of human civilization and have evolved mainly for the survival of the group or society.

Moral values are generally shared values in a society, the degree of sharing these values varies greatly. We may agree more on values like truth, justice, and loyalty than on others. (See operational definitions given in Chapter 1)

2.1.3 Rules and laws

According to Oxford Dictionary, a rule is a statement of what may, must or must not be done in a particular situation. According to Webster's Dictionary, law is a rule of conduct or an action recognized by custom or decreed by a formal enactment, community, or group.

Bourn in Kizza (2007) states that law is an art we can create and model, and contemporary critics define law as an instrument of exercising power.

Fagothey (1959) defines laws as a rule and measure of actions directing them to proper ends. It obliges us to make our conduct conform to the norm of morality. He goes on to divide law into two types:

i. Physical law, which directs non-free irrational beings to uniform action toward their ends by inner necessity of their nature, that is, imposing physical necessity, and
ii. Moral law or natural law, which directs free rational beings toward their ends by imposing obligations on the free will—thus imposing moral necessity.

2.1.4 Principles

Oxford dictionary defines principle as a moral rule or a strong belief that influences ones actions. Principle, is one of those things morality concerns itself with apart from a set of shared rules and duties. This is independent from religion, applicable to all in a group or society, and having no reference to the will or power of any one individual whatever his or her status in that group or society. (Kizza, 2007) In the context of an operational definition with regards to professions, ethics generally refers to those principles and codes of behaviour that guide the conduct of any profession. (Ugbogbo and Atu, 2016)

2.2 E-government

A number of frameworks and models have been developed to describe e-government and the different aspects or components it is made of depending on what the writer wants to explain. A few of them are briefly presented below from the literature reviewed, taking into account the technical difference between e-government and e-govervance. The first two have already been explained in detail earlier in the chapter.

2.2.1 Dimensions

The ITU e-government implementation toolkit gives the dimensions of e-government as

i. Outreach
ii. Governance
iii. Policy and
iv. Infrastructure

The framework uses these four dimensions to describe and understand the realities that influence a country's level of e-government readiness for e-government implementation.

2.2.2 Interactions

On the hand, the UNESCO e-government toolkit for developing countries states that there are primarily four types of interaction which form the foundation of e-government deployment:

i. Government to Government (G2G)
ii. Government to Citizen (G2C)
iii. Government to Business (G2B)
iv. Government to Employee (G2E)

2.2.3 Pillars

According to Sheel and Sheel (2017), the pillars of E Governance are capital, connectivity, competence and content.

i. Capital: E-governance services are capital intensive and to fulfill the motive of speedy and efficient at subsidized rate, further makes it more costly as govt has to bear the major portion of cost.
ii. Connectivity: The very basic purpose of e-governance is to connect citizens with govt which is possible if the services are in reach of each and every one and a large chunk of society is beneficiary.
iii. Competence: Competence is the ability to harness the skills and intelligence of those who are at the planning and implementation level as well as to help govt work in synergy with people, realizing and solving their problems so that they can reap the actual benefits of E Governance.
iv. Content: Content here refers to the availability of services in regional language so as to connect maximum people with E Governance.

On the one hand, Kalam (2006) states that fundamentally, e-Government projects would stand on four key pillars – People, Process, Technology and Resource (PPTR).

On the other hand Kolachalam (2002) identifies the basic structure of e-government as constructed around the following four pillars;

i. Leadership/Vision
ii. Governance/Administration
iii. Integration/Collaboration
iv. Technology/Infrastructure

2.2.4 Implementation phases

Sunitha (2007) notes that there are four (4) phases he calls stages of e-government implementation, these are;

i. Stage one: Cataloguing

   In this stage, government creates a state website, due to demand from external sectors such as citizens, stakeholders as well as employees. At this stage government does not have enough IT experts, therefore go for small projects to reduce the risks of failure.

ii. Stage two: Transaction

   This stage empowers citizens to perform transactions online anytime, serving time of paperwork. Here the demand for e-transaction pushed the government to build online interface directly connected with government system to minimize the interactions with government employees.

iii. Stage three: Vertical integration

At this stage, the focus is on transformation of government services, that is, automating and digitalizing existing processes. However, e-government is not simply putting existing government services online. It requires a re-conceptualization of the government services.

iv. Stage four: Horizontal integration

To achieve the full potential of information technology from citizens' perspective, governments provide one stop service centers, where citizens get more than one service.

The E-Government Handbook for developing countries prepared by the Center for Democracy and Technology (CDT), (2002), divides the process of e-government implementation into three phases. These phases are not dependent on each other, nor need one phase be completed before another can begin, but conceptually they offer three ways to think about the goals of e-government. These are;

a. Phase 1: publish – using ICT to expand access to government information
b. Phase 2: interact – broadening civic participation in government
c. Phase 3 - transact: making government services available online

2.2.5 Application domains

Ndou (2004) argues that the full exploitation and implementation of those complex webs of inter-relationships entails three main application domains for e-government (Heeks, 2001):

a. E-Administration – for automation and computerization of administrative tasks and for realization of strategic connections between internal processes, departments and functions
b. E-Services – to realize connections and interrelationships among governments, citizens, businesses and to deliver automated services

c. E-Citizens and E-Society – to enable relationships and interactions among public agencies, citizens and civil community in general.

2.2.6 Transformational areas

According to Ndou (2004), the existing web definitions of e-government yield to three major components that characterize an e-government framework. These are:

(i) Transformational areas

(ii) Users, stakeholders and their interrelationships, and

(iii) E-government application domains.

In this research, the second component is mentioned in 2.2.2 while the third in 2.2.5. Here we look at the first framework only. Ndou (2004) classifies the e-government transformational areas as

(a) Internal refers to the use of ICT to improve the efficiency of the internal functions and processes of government. For example, e-government connects different departments and agencies, thus making information flow much faster and more easily among different governmental departments.

(b) External refers to how ICT opens up new possibilities for governments to be more transparent to citizens and businesses through dissemination of, and access to, a greater range of information collected and generated by the government.

(c) Relational refers to how ICT adoption may enable fundamental changes in the relationships between the citizens and the state, with implications for the democratic process and structures of the government.

2.3 List of all ethical issues that arise in the information age

As defined in Chapter One, an ethical issue is a problem or situation that requires a person or organization to choose between alternatives that must be evaluated as right (ethical) or wrong (unethical). This is the formal definition of ethical issues adopted throughout this study. In simplistic terms, the researcher defines ethical issues as those issues which lend themselves as matters where an individual, as a moral being, has to engage his or her moral intellect to make a decision as to whether something is right or wrong. Further, a moral being is a free rational being with free will.

Using the proposed theoretical framework (the G2C/G2E Matrix), the literature reviewed brought out the following issues as ethical issues that arise in the use of information technology. This is a compilation put together for the purpose of this research, it may not be exhaustive in itself.

2.3.1 Privacy

According to Jerry Durlak in Kizza (2007), privacy is a human value consisting of four elements he calls rights. He puts these rights into two categories. The first category includes three rights that an individual can use to fence off personal information seekers; the second category contains those rights an individual can use to control the amount and value of personal information given out.

1. Control of external influences:
    - Solitude: the right to be alone without disturbances.
    - Anonymity: the right to have no public personal identity.
    - Intimacy: the right not to be monitored.
2. Control of personal information:

- Reserve*:* the right to control one's personal information including the methods of dissemination of that information.

Quinn defines privacy as a "zone of inaccessibility" that surrounds a person. He notes that one has privacy to the extent that they can control who is allowed into their zone of inaccessibility. For example, you exercise your privacy when you lock the door behind you when using the toilet. You also exercise your privacy when you choose not to tell the clerk at the health club your national identification number. However, privacy is not the same thing as being alone. For example, two people can have a private relationship. It might be a

(i) Physical relationship, in which each person lets the other person become physically close while excluding others, or it might be an

(ii) Intellectual relationship, in which they exchange letters containing private thoughts.

Laudon (2008) notes that the Internet technology has posed new challenges for the protection of individual privacy. Information sent over this vast network of networks may pass through many different computer systems before it reaches its final destination. Each of these systems is capable of monitoring, capturing, and storing communications that pass through it. For instance tools such as cookies, web beacons (web bugs), and spyware using different techniques and methods are capable of gathering information about online users. It is possible to record many online activities, including what searches have been conducted, which Web sites and Web pages have been visited, the online content a person has accessed, and what items that person has inspected or purchased over the Web. Much of this monitoring and tracking of Web site visitors occurs in the background without the visitor's knowledge. It is conducted not just by individual Web sites but by advertising networks.

When we look at privacy from the point of view of outsiders seeking access, the debate revolves around where to draw the line between what is private and what is public (known to all). Stepping over this line and violating someone's privacy is an affront to that person's dignity. (Quinn, 2014) You violate someone's privacy when you treat him or her as a means to an end. Put another way, some things ought not to be known. Suppose a friend invites you to see a cool movie trailer available on the Web. You follow him into the computer lab. He sits down at an available computer and begins to type in his login name and password. While it is his responsibility to keep his password confidential, it is also generally accepted that you ought to avert your eyes when someone is typing in their password. Another person's password is not something that you should know.

2.3.2 Confidentiality

Confidentiality is a subset of data security. According to Singh and Karaulia (2011) any e-governance initiative will remain venerable to security breaches in the absence of a well-articulated security policy. Information security policies are the cornerstone of information security effectiveness. This ethical issue in computing is always considered a subcomponent of data security.

Data Security will help the user to control and secure information from, inadvertent or malicious changes and deletions or unauthorized disclosure. There are three aspects of data security:

(i) Confidentiality: refers to protection of information from unauthorized disclosure e.g. to the press or to release through improper disposal techniques, or to those who are not entitled to have the same.

(ii) Integrity: is about protecting information from unauthorized modification, and ensuring that information, such as a beneficiary list, can be relied upon and is accurate and complete.

(iii) Availability: is to ensure that the information is available when it is required.

2.3.3 Computer crime

Computer crime is also are ethical issue. It is defined as a crime like any other crime, except that in this case the illegal act must involve a computer system either as an object of a crime, an instrument used to commit a crime, or a repository of evidence related to a crime. The acts that fall under this category are considered to be unethical in nature and are criminalized in most societies. These are acts done using computers or computer-related technologies that fall within the limits that the legislature of a state or a nation has specified are considered illegal and may lead to forfeiture of certain civil rights of the perpetrator.

Laudon (2008) notes that widespread use of computers increases opportunities for computer crime and computer abuse. New technologies, including computers, create new opportunities for committing crime by creating new valuable items to steal, new ways to steal them, and new ways to harm others. This is all true in the deployment of e-government.

In the United States, local, state, and federal legislatures have defined such acts to include the following and more:

- Intrusions of the Public Switched Network
- Intrusions into Public Packet Networks
- Network integrity violations
- Privacy violations

- Industrial espionage
- Pirated computer software
- Fraud
- Internet/email abuse
- Using computers or computer technology to commit murder, terrorism, pornography, and hacking. (Kizza, 2007)

Other according to ZICTA include

- Sexting
- Identity theft (ZICTA, 2018)

2.3.3.1 Zambian Laws on Computer crime

Below is a list of the Zambian laws that prescribe what is referred to as computer crime or any such equivalent acts and accompanying sanctions where the provisions are violated;

Computer misuses and crimes (Amendment) Act 2004

Passed against the background that while technological advances have brought immense benefits to society, there are also some negative developments that have come with the computer age. The legislation recognized this fact and it was felt that the existing legal framework at the time could not keep pace with the new moral and ethical dilemmas that technology has posed and there was need for legislation intervention. (Lupiya, 2009)

ICT Act 2009

Enacted to continue the existence of the Communications Authority and rename it ZICTA, provide for the regulation of ICT, facilitate access to ICT, protect the rights and interests of

providers and consumers. It also repealed the Telecommunications and the Radio Communications Acts of 1994.

ECT Act 2009

An Act to develop a safe, secure and effective environment for the consumer, business sector, to conduct and use electronic communications, promote legal certainty and confidence, facilitate the creation of secure communication systems and networks. Also among other provisions establishes the Central Monitoring and Coordination Centre and repeals the Computer misuses and crimes Act of 2004.

ICTAZ Act 20

An Act to establish the Information and Communications Technology Association of Zambia and provide for its functions; provide for the registration of information and communications technology professionals and regulate their professional conduct in the interest of the information and communications technology sector.

Penal Code Act, Cap 87 of the Laws of Zambia

This is a code of laws concerning crimes and offenses and their punishment. (Meriam Webster Dictionary) In Zambia, computer-related fraud has not specifically been legislated against. The Penal Code which was meant to counter traditional fraud has remained un-updated despite the eminent need to have legislation that is technologically accommodative. (Lupiya, 2009)

Copyright and performance rights Act Cap 406 of the Laws of Zambia

This is an Act meant to provide for copyright in literary, musical and artistic works, computer programs, audio-visual works, sound recordings, broadcasts and cable programs; to provide for rights in performances; to repeal the Copyright Act.

2.3.4 Computer decisions

When computers are relied upon to make decisions, a new phenomenon of Artificial Intelligence (AI) is created. According to the Meriam-Webster dictionary Artificial Intelligence is the capability of a machine to imitate intelligent human behavior. (Also see 2.10 on page 60) Nick Bostrom and Eliezer Yudkowsky (2014) note that the possibility of creating thinking machines raises a host of ethical issues. The questions that arise relate both to ensuring that such machines do not harm humans and other morally relevant beings, and to the moral status of the machines themselves.

Maner (1978) authored a Starter Kit on Teaching Computer Ethics. The kit contained curriculum materials and pedagogical advice for university teachers to develop computer ethics courses. It also included suggested course descriptions for university catalogs, a rationale for offering such a course in a university, a list of course objectives, some teaching tips, and discussions of topics like privacy and confidentiality, computer crime, computer decisions, technological dependence and professional codes of ethics. This shows that computer decisions was also identified as an ethical issue in the use of information technology.

2.3.5 Technological dependence (Syndrome)

As indicated above, technological dependence, alongside computer decisions, was identified as an ethical issue by Maner (1978) in his Starter kit. According to Laudon (2008) ethical issues long preceded information technology. Nevertheless, information technology has heightened ethical concerns, taxed existing social arrangements, and made some laws obsolete or severely crippled. There are four key technological trends responsible for these ethical stresses and they are summarized in Table 2.1 below.

Table 2.2: Technology trends that raise ethical issues [*Laudon (2008)*]

TREND	**IMPACT**
Computing power doubles every 18 months	More organizations depend on computer systems for critical operations
Data storage costs rapidly declining	Organizations can easily maintain detailed databases on individuals
Data analysis advances	Companies can analyse vast quantities of data gathered on individuals to develop detailed profiles of individual behavior
Networking advances	Copying data from one location to another and accessing personal data from remote locations are much easier

The doubling of computing power every 18 months has made it possible for most organizations to use information systems for their core production processes. As a result, our dependence on systems and our vulnerability to system errors and poor data quality have increased. Social rules and laws have not yet adjusted to this dependence. Standards for ensuring the accuracy and reliability of information systems (see 2.3.6) are not universally accepted or enforced.

In 1999, Qiao Liang and Wang Xiangsui published a statement in the introduction to a document entitled Unrestricted Warfare: China's Master Plan to Destroy America. The People's Liberation Army printed this document to both trace the strategic and operational successes of the United States' military, but more importantly to highlight its current weaknesses. In a strictly military sense, these vulnerabilities were through a presumed strength, technology. (Carroll, 2014)

2.3.6 Reliability

According to Parnas et al. (1990), reliability of software is the probability that such a software does not encounter an input sequence that leads to failure. A software product, therefore, is reliable if it can continue to function on numerous unpredictable input

sequences. Other measures of reliability include the number of errors in the code. But this also is difficult to take as a good measure because a program with fewer errors is not necessarily more reliable than one with many. Because no system can be certified as error free, including software systems, there have been numerous cases, and will continue to be, in which systems have and will fail the reliability standards.

Twizeyimana and Andersson (2019) in their literature review research work whose aim was to come up with a descriptive conceptual framework that improves the understanding of the public value of e-government observe that reliability is an ethical issue. Below are the cases in point;

By means of a content analysis of each of the 53 articles selected for their study, six (6) overlapping dimensions of the public value of e-government are identified. These are:

(i) Improved public services

(ii) Improved administrative efficiency

(iii) Open Government (OG) capabilities

(iv) Improved ethical behavior and professionalism

(v) Improved trust and confidence in government, and

(vi) Improved social value and well-being.

The generalization of the content analysis results yield to three overarching dimensions of the public value of e-government. They are –

a. Improved Public Services

b. Improved Administration, and

c. Improved Social Value.

This is illustrated in the diagram below;

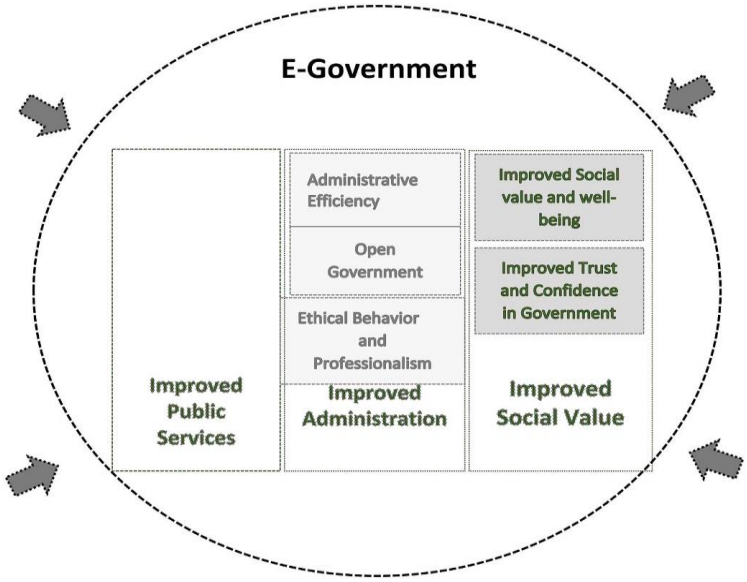

Fig 2.2: Generalization of the six dimensions of the public value of e-government into three main dimensions – a graphical representation [*Twizeyimane and Andersson (2019)*]

The dimension "Improved Trust and Confidence in Government" refers to "social trust", trust that is gained from the extent to which the government secures public information and privacy of citizens and to the public trust, that is, the way public organizations, manage economy, public resources, and delivery of services. Public trust is also gained by providing the public with better access to government information and services (Rose, Persson, & Heeager, 2015; Rose, Persson, Heeager, et al., 2015), and by increasing flexibility, reliability and customer service (Chircu, 2008).

The dimension "Improved Ethical Behavior and Professionalism" is related to "Foundational values" by Rose, Persson, and Heeager (2015). These values are at the backbone of government operations and policies (Rose, Persson, Heeager, and Irani, 2015). They include, but are not limited to, responsibility to the citizens, proper and efficient use of public funds, facilitation of the democratic will, integrity, honesty, fairness, accountability, economy or parsimony, rectitude, legitimacy, rule of law, effectiveness, coherence, adaptability, impartiality, objectivity, trustworthiness, and openness (Bannister & Connolly,

2014; Mkude & Wimmer, 2013; Rose, Persson, & Heeager, 2015; Rose, Persson, Heeager, et al., 2015). Foundational values refer to robustness, reliability, demand for good information for decisions, security, efficiency, effectiveness, better access to government information and services, collaboration, participation, maintaining accurate durable records, durable and competent institutional capacity (Grimsley & Meehan, 2007; Rose, Persson, & Heeager, 2015; Rose, Persson, Heeager, et al., 2015), and decisions by law and authorized policy.

2.3.7 Security

Security is regarded as one of the core values of life. More than a decade later, Moor significantly enhanced his theory of computer ethics. For example, he introduced the notion of 'core values' – such as life, health, happiness, security, resources, opportunities and knowledge – which are so important to the continued survival of a community that essentially all communities must value them. In information technology, security has to do with systems and information security. (Moor 1998)

In general, security can be considered a means to prevent unauthorized access, use, alteration, and theft or physical damage to property. Security involves these three elements:

I. Confidentiality: to prevent unauthorized disclosure of information to third parties. This is important in a number of areas including the disclosure of personal information such as medical, financial, academic, and criminal records.

II. Integrity: to prevent unauthorized modification of files and maintain the status quo. It includes system, information, and personnel integrity. The alteration of information may be caused by a desire for personal gain or a need for revenge.

III. Availability*:* to prevent unauthorized withholding of information from those who need it when they need it.

There are two types of security: physical security, which involves the prevention of access to physical facilitates like computer systems, and information security, which involves the prevention of access to information by encryption, authentication, and other means. The security of both the computer systems and information security is what is today commonly referred to as cyber security. Cyber-security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. (Kaspersky)

2.3.8 Intellectual Property

The computer revolution, by de-materializing (digitizing) artefacts, products and services and transforming them in strings and streams of digits, has profoundly affected concepts such as ownership, intellectual property, copyright, fair sharing and use, as well as voluntary collaboration and open source software there by raising ethical concerns.

Intellectual property is any unique product of the human intellect that has commercial value. Examples of intellectual property are books, songs, movies, paintings, inventions, chemical formulas, and computer programs. (Quinn, 2014)

Bernd Carsten Stahl in Floridi (2010) notes that intellectual property is a pervasive issue of ethical relevance that touches many aspects of modern societies. Questions include whether software or content can or should be owned, how they can be protected and how protection mechanisms can be enforced.

Locke (1988) developed an influential theory of property rights. In The Second Treatise of Government, Locke makes the following case for a natural right to property. First, people have a right to property in their own person. Nobody has a right to the person of anybody

else. Second, people have a right to their own labor. The work that people perform should be to their own benefit. Third, people have a right to those things that they have removed from Nature through their own labor. This relates to physical property, Quinn (2014) extends this argument to intellectual property, he writes that

2.3.9 Anonymity

As observed earlier anonymity is among the four elements of human value under piracy. Anonymity is defined as the right to have no public personal identity (Kizza, 2007).

Floridi (2008) in his paper Foundations of Information Ethics, postulates that being informed is not always a blessing and might sometimes be morally wrong or dangerous. One may need to lack (or intentionally preclude him or herself from accessing) some information in order to achieve morally desirable goals, such as protecting anonymity, enhancing fair treatment or implementing unbiased evaluation. This he demonstrates using figure 2.4 below.

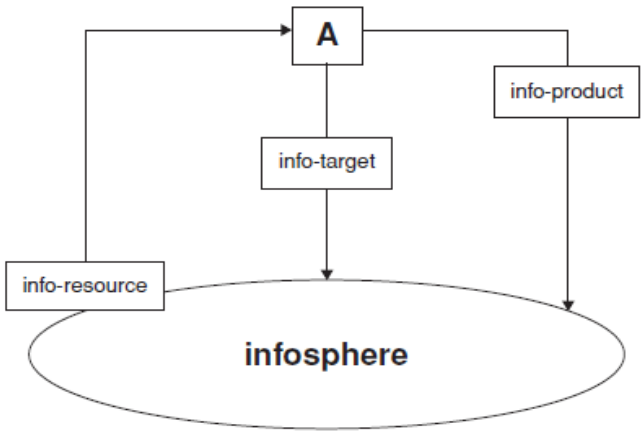

Fig 2.3: The 'External' R (esource) P (roduct) T (arget) Model [*Floridi (2008)*]

He supposes that if *A* is interested in pursuing whatever she considers her best course of action, given her predicament. We shall assume that *A*'s evaluations and actions have some

moral value, but no specific value needs to be introduced. Intuitively, *A* can use some information (information as a *resource*) to generate some other information (information as a *product*) and in so doing affect her informational environment (information as *target*). Famously, Rawls' 'veil of ignorance' exploits precisely this aspect of information-as-a-resource in order to develop an impartial approach to justice (Rawls 1999). For the (sometimes explicit and conscious) withdrawal of information can often make a significant difference. This is the case in the right to remain anonymous as a whistle-blower as mentioned in the case of Shi Tao by John Sullins in Floridi (2010).

In the same vain, the ethical test of anonymity can presumably be tested in this scenario; an anonymous whistle-blower seeks anonymity in order to protect herself from reprisal, for example, being fired or harassed. At the same time, such anonymity could provide space for slanderous or false charges of incompetence by a disgruntled employee.

2.3.10 Computer technology for people living with disabilities

Lazarus (2007) notes that although the current level of access to technology is a recent phenomenon, most people take these conveniences for granted. However, technology may be a mixed blessing for persons with disabilities and pose ethical dilemmas for developers who wish to provide global access for all, thereby becoming an ethical issue.

A U.S. law known as "Section 508" requires that each Federal agency's electronic and information technology must be accessible to people with disabilities. The Center for Information Technology Accommodation (CITA), in the U.S. General Services Administration, is responsible for educating Federal employees and designing the infrastructure necessary to support Section 508 implementation. (CTD, 2002)

Also, for ensuring a wider reach and coverage amongst the common citizens, it is suggested that a portal should have versions in multiple regional languages. Also, an emphasis has to be given to ensuring 'universal' accessibility of the portal. This would mean that the portal should be accessible through multiple devices (the mobile devices, hand held devices, PDAs etc.) as well as to the entire cross-section of target audience, including people with certain disabilities. (UNESCO, 2005)

Accessibility refers to the extent to which the portal and its contents are available to a wide range of users with varied levels of physical capabilities/skills and technologies. A portal being universally accessible would imply that a broad range of software, hardware and audiences, including physically challenged citizens can not only access the online content and services on the portal but are also able to actually make use of it. The World Wide Web Consortium's (W3C) Web Accessibility Initiative (WAI) is an internationally agreed recommendation for website accessibility for people with special needs and it is expected of the Government websites to follow these standards. It is important that reasonable steps are taken to sensitize the developers to alter practices, policies and procedures that make it impossible or unreasonably difficult for people with disabilities to access or use the web portal.

Some learners have used speech recognition systems successfully for their studies and for examinations, and the use of this technology has helped them to overcome their physical disabilities and go on to higher education Paul (2003) in Handbook of Research on E-Services in the Public Sector: E-Government Strategies and Advancements.

2.3.11 Digital divide

When considered a universal resource that could be used to provide a public service in e-government dispensation, it becomes an ethical issue when ICT tools cannot be afforded by all citizens intended to be served by their government. The questions that arise are:

- Is there a "digital divide" separating society into "haves" and "have nots"?
- Is information technology widening the gap between rich and poor?

The term "digital divide" refers to the opportunity gap brought about because some people do not have access to modern information technology, particularly the Internet.

In other words, digital divide refers to the situation in which some people have access to modern information technology while others do not. The underlying assumption motivating the term is that people who use cell phones, computers, and the Internet have opportunities denied to people without access to these devices. The idea of a digital divide became popular in the mid-1990s with the rapid growth in popularity of the World Wide Web. According to Pippa Norris in Quinn (2014), the digital divide has two fundamentally different dimensions. The global divide refers to the disparity in Internet access between more industrialized and less industrialized nations. The social divide refers to the difference in access between the rich and poor within a particular country.

In 1994, the U.S Commerce Department's National Telecommunications and Information Administration (NTIA) published a report, "Falling Through the Net", commonly referred to as NTIA I. (Kizza, 2007) The NTIA I report used the Information Communications Technologies (ICT) access indicator, one of the many digital divide indicators, to highlight sectors of the U.S population that were technologically deprived. Since then the digital divide debate has been raging, centred on a number of key critical issues including:

- whether there is such a thing as a digital divide,
- indicators that should be used to measure such a divide if it exists, and
- The best ways to close such a divide.

In general, the study of the digital divide involves the study of the impact on society's social, economic, political, and cultural institutions from communication technologies such as radio, television, the press, post offices, fixed and cellular telephones, fax machines, airports, computers, and connectivity to the Internet. However, the NTIA I itself focused only on a few more modern communication technologies, these are telephones, personal computers, and connectivity to the Internet. There are five indicators of the digital divide, namely, access, technology, humanware (human capacity), infrastructure, and enabling environment. These are summarized as follows;

1. Access
    a. Geography
    b. Income
    c. Ethnicity
    d. Age
    e. Education
2. Technology
    a. Hardware
    b. Software
3. Humanware (human capacity)
4. Infrastructure
5. Enabling Environment

a. Politics

b. Public policy and management styles

Another ethical issue impacted by the increasing use of online campaigning is the long-standing concern that the use of e-democracy technologies reinforces the digital divide; the idea that these technologies unduly advantage the societal elite and leave the less privileged even more isolated and excluded. (Fraunholz & Unnithan, 2008) While access to the Internet is steadily increasing in most liberal democracies, political players still need to devise strategies that ensure that all citizens can participate fairly and freely in democratic processes. (Al Ajeeli and Al-Bastaki, 2011)

2.3.12 Trust

The Oxford dictionary defines trust as the belief that somebody or something is good, sincere, honest, etc. and will not try to harm or trick you. Having these moral values in its definition qualifies trust as an ethical issue considered for this study.

Designing and implementing more trustworthy government e-services is an important issue, because, the governmental information is often so sensitive. Furthermore, security has an important role in trust formation of citizens and their adoption of e-government. (Sharma Gajendra, Bao Xi and Qiang Wang, 2012)

Better administration leads to effective management of delivery of governmental services and this comes from managing e-governance ethical processes. According to Chopra and Wallace (2003) trust is considered a crucial element with regard to social capital, and exists on four levels: the individual (psychological), the interpersonal (one to another), the relational (social glue) and the societal (functioning). Some important ethical issues connected to e-governance are e-communication legislation, e-commerce legislation, e-

procurement legislation and database legislation. The e-governance implication needs to build the trust of people. It needs to make sure that the data and transactions of the information are secure.

The information shared by the public should also remain safe and the privacy of the people needs to be preserved. Whenever an individual gets into any transaction with a government agency, he discloses a lot of personal information, which can be misused by the private sector and anti-social elements. (Gajendra Sharma, 2014)

2.3.13 Legitimacy

The issue of legitimacy in e-government is discussed when looking at the use of ICT in democratic dispensation in a new concept referred to as e-democracy. Stahl (2005) discusses one aspect of the relationship that the use of information and communication technology (ICT) in business has with the use of ICT in government and administration. He argues that democracies rely on their ethical legitimacy and that framing e-government and e-democracy in commercial terms can jeopardize this legitimacy. He goes on to state that this approach not only endangers the success of e-government and e-democracy but may even threaten the basis of the moral legitimacy of democratic forms of government.

The central problem is that the conceptualization of humans differs fundamentally between the business world and politics. In business people are most importantly consumers whereas in democracy, people are predominantly citizens. The danger of the commercial paradigm is that it implies that citizens can be reduced to consumers. This change of the conceptualization of humans creates a change from e-democracy to e-government, it excludes certain members from inclusion, and it generally affects the character of democracy. This, it will be argued, threatens the moral legitimacy of democracy which is

the central basis of its acceptability and therefore of its success. The conclusion will therefore be that politicians as well as information systems professionals must make sure that they keep the sometimes fine line between business processes and political processes in mind in order to avoid a failure of the (political as well as technical) system and retain its legitimacy.

There are different reasons why democracy is linked to ethics and morality. Maybe the most obvious one is that it is a system that distributes power. Power affects our moral rights and obligations, the way we can and should behave, and it is also of theoretical and reflective importance. The most important aspect of ethics and power in democracies is that democratic processes give power legitimacy. Power as the ability to make others do one's bidding is a necessary part of any community and it can only be held if the affected parties believe it to be justified and legitimate. In a post-metaphysical society the source of legitimacy of power can apparently only come from the assumption that democratic processes, albeit fallible, create the most reasonable results that can be expected (Habermas, 1998).

2.3.14 Internet addiction

According to Michael Quinn (2014), people who use the Internet excessively can harm themselves and others for whom they are responsible. For this reason, excessive Internet use is a moral issue. People who use the Internet excessively can harm themselves and others for whom they are responsible. For this reason, excessive Internet use is a moral issue. Kantianism, utilitarianism, and social contract theory, which are ethical theories, all share the Enlightenment view that individuals, as rational beings, have the capacity and the obligation to use their critical judgment to govern their lives. Kant held that addiction is a

vice, because it's wrong to allow your bodily desires to dominate your mind. Mill (1993) in Quinn (2014) maintained that some pleasures are more valuable than others and that people have the obligation to help each other distinguish better pleasures from worse ones. Some people spend a great deal of time online, but psychologists disagree whether it is possible to become addicted to the Internet.

Samson and Keen (2006) believe that pornography is among phenomena which are categorized under Internet addiction including net gaming, cyber-relational addiction, information overload, computer addiction and cyber-sexual addiction.

2.3.15 Fairness

According to Reynolds (2014), fairness is a virtue. A virtue is a particular good quality or habit (virtue). Virtues are only possessed by human beings by virtue of being moral beings as they are capable of making moral decisions. One is said to be fair if they possess a quality of treating people equally or in a way that is reasonable.

In the advent of artificial intelligence and machine learning, where automated information systems are replacing humans and given responsibility once performed by human beings to make decisions. The ability of the systems to perform such duties with fairness is under scrutiny. Therefore, fairness is considered an ethical issue.

2.4 E-government ethics

Various frameworks have been used by scholars of e-government to understand the ethical issues that arise in the implementation of e-government.

Mullen and Horner (2004) note in their evaluative framework that the extent to which types of moral wrongdoing are classified relate specifically to the technologies used. There framework identifies four categories of ethical issues:

i. Those related to electronic environments;

ii. Those dependent on electronic environments;

iii. Those determined by electronic environments; and

iv. Those specific to electronic environments.

Table 2.3: Evaluative framework of ethical problems for e-Government [*Horner & Mullen (2004)*]

Evaluative framework of ethical problems for e-Government	
Related issues are ones where electronic environment is neither necessary or sufficient for ethical problems to arise	**Dependent issues** are ones where electronic environment is necessary but not sufficient for ethical problems to arise
Determined issues are ones where electronic environment is sufficient but not necessary for ethical problems to arise	**Specific issues** are ones where electronic environment is both necessary and sufficient for problems to arise and thus creates unique new moral issues

Ramadhan et al (2011), classify ethics in three branches and these are metaethics, normative ethics and applied ethics. On applied ethics, they note that there are three applied ethics, in the world of computers science, which they used as a reference in their study, that is, computer ethics, information ethics, and cyber ethics.

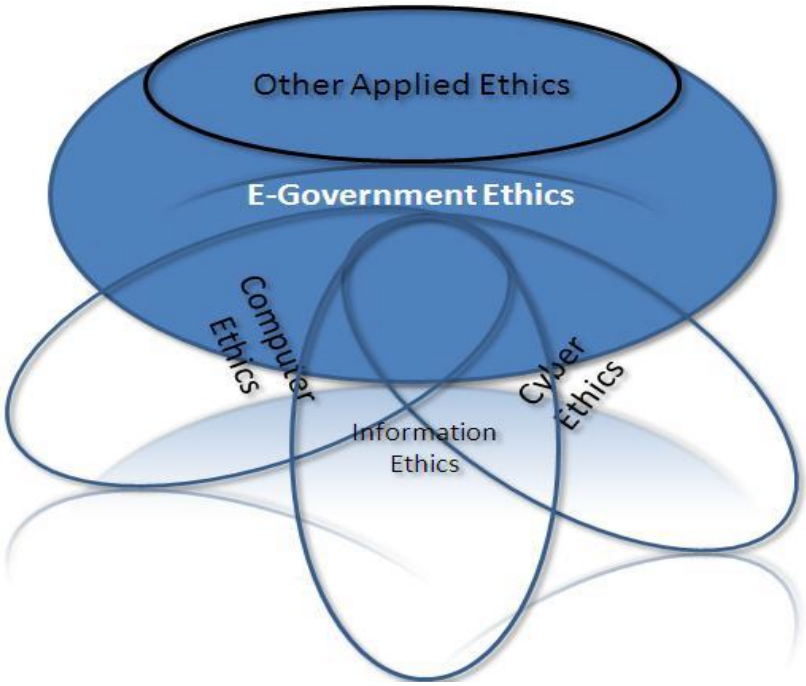

Fig 2.4: e-Government ethics position related to other applied ethics [*Ramadhan et al (2011)*]

2.5 A Review of Zambia's e-Government Master plan

The e-government master plan developed earlier but launched by the Zambian government in 2019, among other things provides the scope of the e-government projects. The scope is holistically divided into broad phases of five years each. The initial five years are very important for laying a solid impeccable foundation for the development and sustenance of e-Government in Zambia. Therefore phase one (2016 – 2020) will be focused on the fundamental ICT pillars which according to the Beuchuma Model include;

(i) The governance infrastructure,

(ii) The technical infrastructure and

(iii) The knowledge infrastructure for the ICT Infrastructure as shown in figures 1 -4.

In the same phase systems integration and e-services will be implemented according to the information architecture pillars by Open Group Architecture Framework (TOGAF) which are; business architecture, data architecture, application architecture and technology architecture.

Fig 2.5: Governance Infrastructure [*SMART Zambia (2015)*]

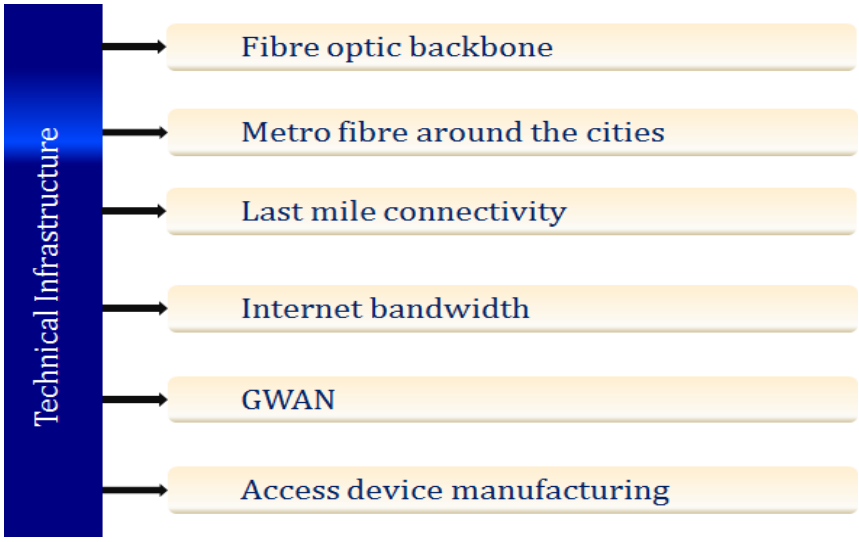

Fig 2.6: Technical Infrastructure [*SMART Zambia (2015)*]

Fig 2.7: Knowledge Infrastructure [*SMART Zambia (2015)*]

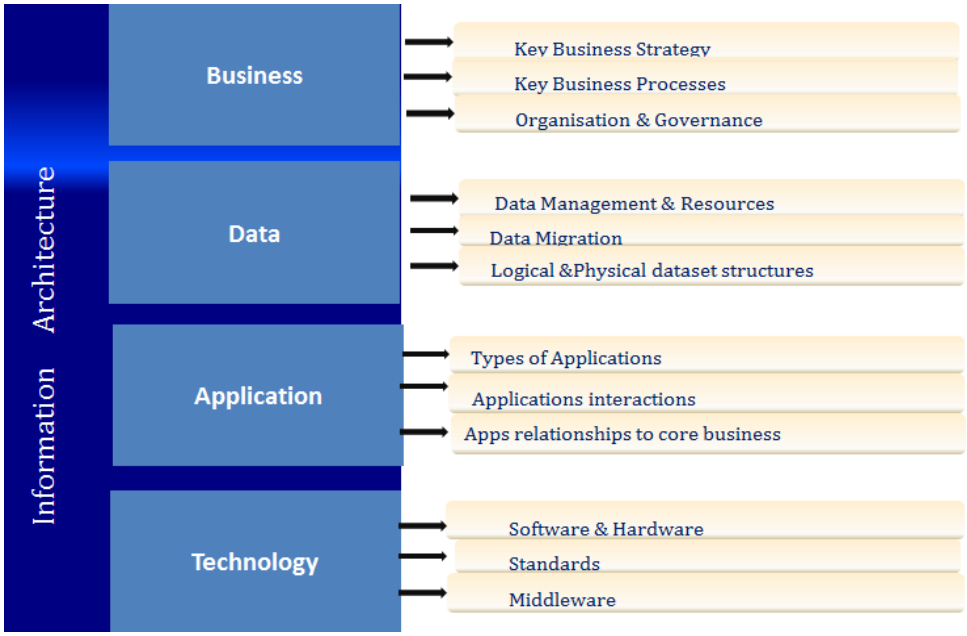

Fig 2.8: Information Architecture [*SMART Zambia (2015)*]

The master plan also adopts the Gartner e-Government maturity model. According to this model, the availability of web services for governments and its subsidiaries follows a systematic pattern as demonstrated in Figure 2.11 below;

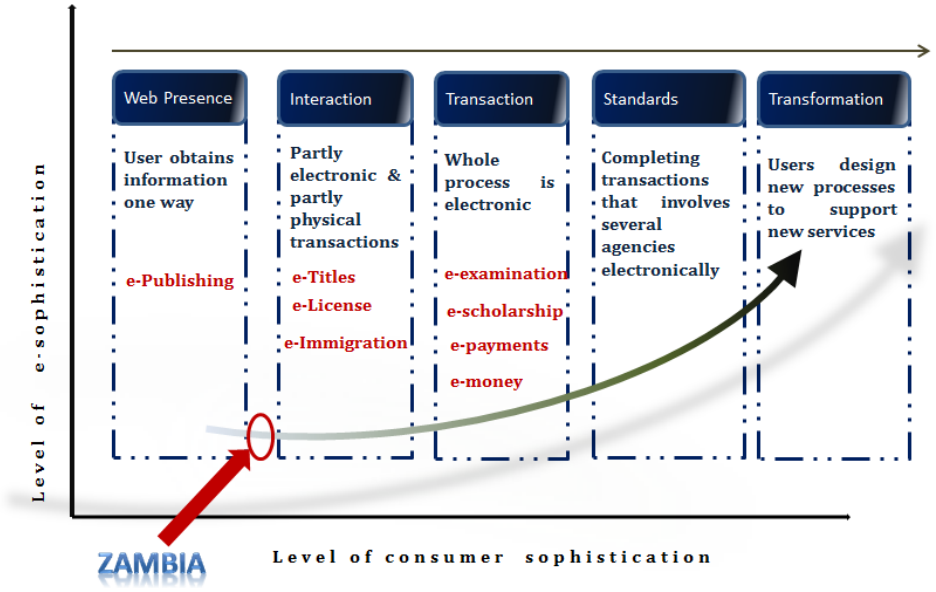

Fig 2.9: Zambia's Gartner e-Government Maturity Model Position [*SMART Zambia (2015)*]

In an e-Government Assessment Report of the recently conducted survey, Zambia is oscillating between web presence and interaction. (SMART Zambia, 2016) The web presence phase merely ensures that government displays its information on widely accessible web portals. This is already happening through tender advertisements and information sharing to citizens. The second phase is interaction. During this phase citizens are able to start an electronic transaction but they have to complete it through manual interventions. Examples here include acquisition of drivers' licenses, electronic taxes and immigration documents.

2.6 Policy formulation and Systems Design

According to Goldkuhl (2012), the development of policies must precede the design of any systems for e-government. He demonstrates this in the use of the PDE model. Meaning Policy Design Effects in that order of manifestation in the implementation of e-government. Policy is what is shaped in implementation and use of processes. Design can mean the design process, that is, all the design activities. Design can also mean design product, that is, the created IT artefact

and other intended design products. This means that the statement "from policy to design and effects" is an abbreviation of the longer statement "from policy to design process, design products and effects". Effects do not occur directly from the designed product, but rather from the use of the products/artefacts.

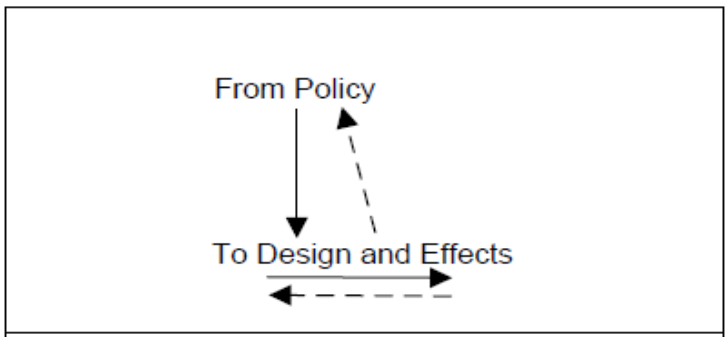

Fig 2.10: The e-government PDE model [*Goldkuhl (2012)*]

Policy precedes design which in turn precedes the effects experienced in the use of the product or artefact. The concept of policy includes laws, regulations, policy declarations, work practice goals and other statements of normative kind. The concept of design in this model is equivocal. Design can mean design process, that is, design activities. Design can also mean design product, that is, the created IT artefact and other intended design products. This means that the statement "from policy to design and effects" is an abbreviation of the longer statement "from policy to design process, design products and effects". Effects do not occur directly from the designed product, but rather from the use of the products/artefacts. An even more comprehensive statement reads as follows: "from policy to design process, design products and their uses leading to effects". He further postulates that ontologically, there is a chain from collective values (policy) via design activities to designed artefact that can give rise to effects through use.

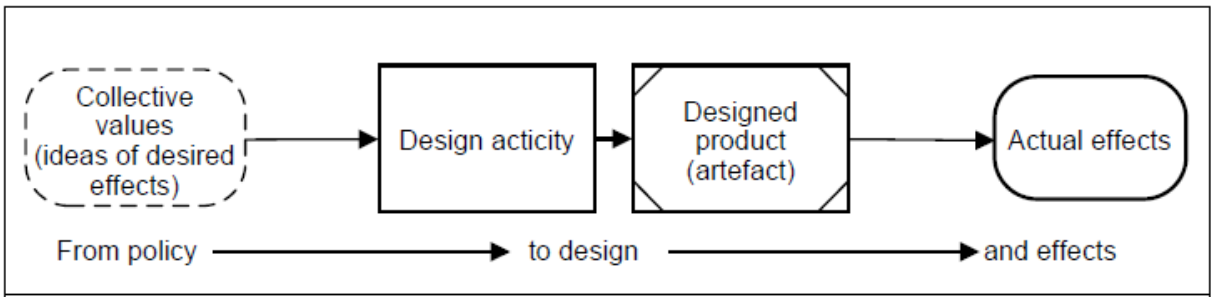

Fig 2.11: From policy to design and effects: Ontological chain [*Goldkuhl (2012)*]

2.7 National ICT Policy, NDPs, ICT Acts and e-Government bills

Zambia's efforts to implement e-government can be traced to the development of the National ICT Policy in 2006. The policy strongly emphasizes the creation of an innovative, market responsive, highly competitive, coordinated and well-regulated ICT industry. The Policy is anchored on thirteen focus areas namely; Human Resources Development, Agriculture, Tourism, Telecommunication infrastructure, Environment and Natural Resources, Education, Health, e-Commerce, e-Government, Youth and Women, Security in information society, Access, media, content and culture and Information and Communication Technology services.

Apart from the National ICT Policy, The NISP, 2015-2020 was developed. This was aimed at operationalizing the ICT Policy of 2006 and ensure integration of ICTs into all sectors of the economy. The Strategy provides a hierarchy of responsibilities, properly focused, time bound for ICT development and a roadmap presenting a series of stages towards achieving the vision and smart targets.

In addition, in the consecutive National Development Plans, The ICT Sector has been recognized as a growth sector in the fifth National Development Plan, (2006-2010) and Sixth National Development Plan (including its subsequent revision 2011-2015 and 2013-2016). The sector was classified as an economic sector able to facilitate and contribute to the growth of the economy.

The Revised Sixth National development plan focusses on ICT Infrastructure, electronic services and Human Resources Skills development.

The following are the Acts that currently govern the ICT sector in Zambia.

(i) **Information and Communication Technology Act No. 15 of 2009**

The Act provides for the economic and technical regulation of information and communication technology; facilitates access to ICTs; "protects the rights and interests of service providers and consumers"; and regulates and manages radio spectrum. The ICT Act also renamed the CAZ to the Zambia ICT Authority (ZICTA). (ICT Act, 2009)

(ii) **Electronic Communications and Transaction Act No. 21 of 2009**

The ECT Act, 2009 provides for the development of a safe, secure and effective environment for the consumer, business sector and the Government to conduct and use electronic communications; promotes legal certainty and confidence, and encourages investment and innovation in the electronic communications industry; facilitates the creation of secure communication systems and networks; and allows the legal interception of electronic communications and admissibility of intercepted communications. (ECT Act, 2009)

(iii) **Information and Communications Technology Association of Zambia Act No. 7 of 2018**

Recently also, the Zambian parliament passed the ICTAZ Act, to provide for the establishment of the Information and Communications Technology Association of Zambia and provide for its functions; provide for the registration of information and communications technology professionals and regulate their professional conduct in the interest of the information and communications technology sector. (ICTAZ Act, 2018)

There are 17 statutory instruments to regulate the ICT sector and some of these include;

a. **Universal Access and Service fund Regulation No.38, 2012**

   In order to promote the widespread availability and usage of electronic communication services throughout Zambia, and to bridge the digital divide between urban, peri-urban and rural areas, Parliament in 2009 passed the Information and Communications Technology (ICT) Act No 15 of 2009. The ICT act established a Universal Access and Service Fund to address the provision of electronic communications services in un-served or under-served areas and communities. The Ministry in June 2012 issued statutory Instrument No. 38 of 2012 to guide the operation of the fund.

b. **Access Regulation, 2013**

   Additionally, a Statutory Instrument on Interconnection, Co-location and Access was issued to provide a legal and regulatory framework for interconnecting and sharing of ICT infrastructure amongst the operators to support growth of the sector, to avoid duplication of infrastructure, to ensure equitable access and to ensure delivery of efficient and affordable services to the customers.

The implications of the legal environmental analysis are:

a. New governance structure that helps to achieve easy service delivery to citizens
b. Better management of e-Government
c. Better control of cybercrimes and e-justice system
d. Better operating business environment for ICT entrepreneurial talent nurturing and growth

In addition, currently the ECT Act, 2009 combines Cyber security and e-Commerce/e-Government provisions. It is earmarked for review and replacement with four new Bills namely;

Cyber Security Bill, E-Government Bill, Electronic Communication Transaction Bill and Data Protection Bill.

2.8 E-government, e-governance, e-democracy and e-participation

In the literature reviewed, a difference in the above terms is given as follows;

E-government is a means for governments to use the most innovative ICTs through electronic networks with more convenient access to government information and services while E-governance is the application of information and communication technology (ICT) for delivering government services, exchange of information and communication between government and public. (Sharma et al, 2012)

Apart from e-government and e-governance, it is important to understand the concept of e-democracy, which is a natural extension of e-governance. E-democracy refers to the processes and structures that encompass all forms of electronic interaction between Government (elected) and the Citizen (electorate). (UNESCO, 2005).

E-participation refers to the ICT-supported participation and processes involved in government and governance. Processes include administration, service delivery, decision making and policy making. E-participation is the use of ICTs to broaden and deepen political participation by enabling people to connect with one another and with their elected representatives. E-participation is very crucial for any e-governance initiative. (Sharma, 2014)

2.9 E-government in service delivery

The term service delivery finds itself as part of the definition of e-government in many definitions. Example is one given by Azeta et al in Handbook of Research on e-Services where E-Government is defined as the use of Information and Communication Technologies (ICT) to

support government operations and service delivery in a responsive and cost-effective manner. In South Africa for instance, the Internet is perceived as an instrument to enhance service delivery performance in the public service. Transformation is what e-Government is all about, and with Internet applications powering streamlined service delivery and supported by the best staff and IT infrastructure, governments will evolve into new enterprises that bear no resemblance to their structure today. (Deloitte Consulting, 2000)

A citizen-centric criteria-based definition of e-government is required to help e-government policy makers and implementers in introducing and following up introduction of e-government for improved public service delivery. (Misra, 2006)

2.10 Value Sensitive Design (VSD)

Batya Friedman, Peter Kahn, and Alan Borning studied the concept of "Value Sensitive Design and Information Systems." The authors note that value sensitive design (VSD) is a theoretically grounded approach to the design of technology that accounts for human values in a "principled and comprehensive manner throughout the design process." (Himma and Tavani, 2008) It also includes a tripartite methodology, consisting of conceptual, empirical, and technical investigations. They explicate Value Sensitive Design by drawing on three case studies. The first study concerns information and control of web browser cookies, implicating the value of informed consent. The second study concerns using high-definition plasma displays in an office environment to provide a "window" to the outside world, implicating the values of physical and psychological well-being and privacy in public spaces. The third study concerns an integrated land use, transportation, and environmental simulation system to support public deliberation and debate on major land use and transportation decisions, implicating the values of fairness, accountability, and support for the democratic process, as well as a highly diverse range of

values that might be held by different stakeholders, such as environmental sustainability, opportunities for business expansion, or walkable neighbourhoods.

Looking on the first study of Cookies and Informed Consent in Web Browsers alone in line with ethical concerns that arise in the use of ICTs; Informed consent provides a critical protection for privacy, and supports other human values such as autonomy and trust. Yet currently there is a mismatch between industry practice and the public's interest. According to a recent report from the Federal Trade Commission of 2000, for example, 59% of Web sites that collect personal identifying information neither inform Internet users that they are collecting such information nor seek the user's consent. Yet, according to a Harris poll of 2000, 88% of users want sites to garner their consent in such situations. Against this backdrop, Friedman, Felten, and their colleagues (Friedman et al., 2000; Millett et al., 2001) sought to design web-based interactions that support informed consent in a web browser through the development of new technical mechanisms for cookie management. This project was an early proof-of-concept project for Value Sensitive Design (VSD).

2.11 Ethics in Artificial Intelligence

Artificial Intelligence (AI) refers to the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions. The term may also be applied to any machine that exhibits traits associated with a human mind such as learning and problem-solving. (Frankenfield, 2019)

The possibility of creating thinking machines raises a host of ethical issues. These questions relate both to ensuring that such machines do not harm humans and other morally relevant beings, and to the moral status of the machines themselves. AI algorithms play an increasingly large role in modern society, though usually not labeled "AI." Designing a robot arm to avoid

crushing stray humans is no more morally fraught than designing a flame-retardant sofa. It involves new programming challenges, but no new ethical challenges. But when AI algorithms take on cognitive work with social dimensions-cognitive tasks previously performed by humans—the AI algorithm inherits the social requirements. Responsibility, transparency, auditability, incorruptibility, predictability are among the list of issue to be looked at when designing AI machines. This list of criteria is by no means exhaustive, but it serves as a small sample of what an increasingly computerized society should be thinking about. (Bostrom and Yudkowsky, 2014)

2.12 Professional regulation

Professional regulation is another interesting area in line with this study of ethics and their impact on e-government implementation. It falls in the G2E interactions of e-government. According to Loui and Miller (2008) the obligations of computing professionals are similar to the obligations of other technical professionals, such as civil engineers. Taken together, these professional obligations are called professional ethics. Ethical obligations have been studied by philosophers and have been articulated by religious leaders for many years. Within the discipline of philosophy, ethics encompasses the study of the actions that a responsible individual should choose, the values that an honorable individual should espouse, and the character that a virtuous individual should have. For example, everyone should be honest, fair, kind, civil, respectful, and trustworthy.

There have been debates for and against recognition of computing as a profession. Kizza (2007) notes that there are three basic professional requirements, namely:

1. A set of highly developed skills and deep knowledge of the domain.
2. Autonomy.

3. Observance of a code of conduct.

Further, he states that professionalism is supported by four pillars: commitment, integrity, responsibility, and accountability.

Computing professionals perform a variety of tasks: They write specifications for new computer systems, they design instruction pipelines for superscalar processors, they diagnose timing anomalies in embedded systems, they test and validate software systems, they restructure the back-end databases of inventory systems, they analyse packet traffic in local area networks, and they recommend security policies for medical information systems. Computing professionals are obligated to perform these tasks conscientiously because their decisions affect the performance and functionality of computer systems, which in turn affect the welfare of the systems' users directly and that of other people less directly. For example, the software that controls the automatic transmission of an automobile should minimize gasoline consumption and, more important, ensure the safety of the driver, any passengers, other drivers, and pedestrians.

2.13 Case reviews

2.13.1 The Case of South Africa

E-government in South Africa is at a formative stage and a snapshot of progress is taken by asking the 10 questions posed by the "Roadmap for E-government". There is a strong political will driving the vision and the readiness assessment discusses legal frameworks, governance models, infrastructure and human resource development as key success factors. Alignment of projects with the vision is demonstrated through a number of case studies showcasing innovation in service delivery and customer focus. The crucial issues of corruption, human resource development and monitoring and evaluation are highlighted.

The Roadmap, developed by the Pacific Council on International Policy, seeks to leverage e-government lessons already learned in the developing world to maximize the chances of success for future projects. The "Roadmap for E-government" highlights issues and problems common to e-government efforts. These 10 questions provide indicators to guide e-government implementation.

The Roadmap presents ten questions that e-government practitioners from around the world (including South Africa) believe are crucial to successfully conceiving, planning, managing and measuring e-government. The Roadmap Working Group suggests that e-government officials ask themselves these ten questions before they embark on the e-government path.

The 10 Questions:

1. Why are we pursuing e-government?
2. Do we have a clear vision and priorities for e-government?
3. What kind of e-government are we ready for?
4. Is there enough political will to lead the e-government effort?

5. Are we selecting e-government projects in the best way?
6. How should we plan and manage e-government projects?
7. How will we overcome resistance from within the government?
8. How will we measure and communicate progress? How will we know if we are failing?
9. What should our relationship be with the private sector?
10. How can e-government improve citizen participation in public affairs?

As can be seen, like many other e-government endeavours, the literature reviewed show that South Africa's e-government programme is no exception; Ethical issues that arise in e-government, the measures how, especially the design of systems, to address them elude the policy makers and technocrats at this initial but critical stage of planning. The emphasis is much on the techne (infrastructure) and very little to do with the phronesis (ethics).

2.13.2 The Case of Rwanda

Rwanda is a country with high ambitions regarding ICTs and where e-government is one of the priority areas. According to the Ministry of Information Technology and Communication (MITEC) previously designated as the Ministry of Youth and ICT (MYICT), ICTs in Rwanda are expected to enable the country in achieving its Vision 2020 of transforming the country from a Least Developed Country to a middle-income country (MITEC, 2015, MYICT, 2015). The approach is to adopt ICTs as a means to facilitate access to information and services which in turn would yield a dynamic and knowledge-based economy MITEC (2015;2016;2017), MYICT (2015), and Twizeyimana (2017). As Rwanda is concerned, considerable efforts have been put in place for ICT and its development in the country. These efforts are documented in policy documents such as the National Information Communication Infrastructure plan [2000 – 2015] and the Smart Rwanda Master Plan [2016 – 2020]. In the NICI Plan I to III [2000-2015] the target was to put the legal and regulatory framework in place and build a basic ICT infrastructure MITEC (2015; 2016; 2017) and MYICT (2015). The major infrastructure consists of telecommunication networks, a national fibre optic backbone, a submarine cable, and an integrated national data centre. In the current era of the Smart Rwanda Master Plan [2016 – 2020], the focus is on digitalizing the government towards a 24/7 self-service, "cash-less" and "paper-less" government; with 95% of all government services transacted online by 2018 MITEC (2015;2016;2017), MYICT (2015), and Twizeyimana (2017). At the time of writing, the IREMBO platform is considered the core platform for e-government in Rwanda. The IREMBO project is an initiative by the Government of Rwanda envisioned to digitalize all public services into a single window platform called “IREMBO” (a local term that would mean “Gateway” in English or "Porte d'entrée" in French). In their wish for a solution to inefficient manual

processes, delays in service delivery, long queues and bottleneck in service delivery, the government of Rwanda has entered into a public private partnership (PPP) with the private company Rwanda Online Platform Ltd (henceforth referred to as ROL) for the digitalization of government-to-citizens (G2C) and government-to-business (G2B) services MITEC (2015). The private partner - ROL is given a BOT (Build, Operate, and Transfer) agreement for the IREMBO platform that is envisioned a one-stop-shop for G2C and G2B e-government in Rwanda (Twizeyimana, 2017).

Like their counterpart earlier reviewed, the case is no different for Rwanda. Very little is mentioned in their planning stage about how they intend to tackle ethical issues that may arise in the implementation of e-government. The concept of ethical issues is almost if not non-existence. The techne overshadows the phronesis.

2.14 The gaps identified in the literature reviewed

(i) No literature reviewed, identifies the ethical issues based on the formal definition of what an ethical issue is

(ii) Little attempt is made to identify all the ethical issues that arise in the use of information technology from the ethical context

(iii) Little literature addresses the design of systems in e-government purely from an ethical point of view and absolutely none was come across on Zambia e-government

(iv) No framework for identifying the ethical issues on the user, system and designer perspective use come across.

2.15 Chapter Summary

This chapter has analysed some of the literature on e-government implementation and the definitions of terms such as values, morals, morality and ethics. It also reviewed the e-government implementation in Zambia and the Zambian legislative instruments establishing the legal framework for ICT sector and e-government and how these address any ethical issues that arise in e-government implementation. The chapter further defined what in this study ethical issues are and outlined some identified in the literature reviewed. Furthermore, specific cases of e-government in developing countries in Africa with in relation to how they have implemented e-government and addressed ethical issues if any.

CHAPTER 3

3.0 Methodology of the Study

The methodology that was used through this research work was essentially an examination through literature searches and the analysis of data collected from the field through questionnaires and interviews. The data sources did contribute to the objectives resulting in conclusions and recommendations being drawn from the critical analysis of the collected data.

A methodology is the rationale for the research approach, and the lens through which the analysis occurs. Said another way, a methodology describes the “general research strategy that outlines the way in which the research is to be undertaken. The methodology that was used in this study is participatory. The researcher is also part of the community that was researched on. The methodology of this study derives from the post-positivist paradigm which is based on a philosophy that scientific knowledge in social science is also subjective and that this knowledge may be constructed reality by the researcher.

3.1 Research Approach and Design

Information systems are sociotechnical systems. (Laudon, 2008) Although they are composed of machines, devices, and "hard" physical technology, they require substantial social, organizational, and intellectual investments to make them work properly. Therefore, due to its nature as a socio technical subject, a post-positivism approach was found appropriate to be used as a paradigm for this study. The post positivist paradigm suggests among other things that reality is partly objective and subjective but additionally is experiential.

The mixed method approach was employed during the research in order to get the benefits of both qualitative and quantitative research designs. The research used both primary and secondary data sources and involved the collecting of data using self-administered questionnaires. The questionnaires were designed with reference to the literature reviewed on the Impact of Ethical Issues on e-government Implementation.

The respondents among them policy makers, analysts, regulators, implementers in the ICT industry from various sectors, that is, public and private, as well as ordinary citizens as consumers were the primary sources of data. Published and unpublished books and articles formed the secondary data sources. The primary sources were analysed based on the facts that were presented in various articles and books that have covered similar topics. An online questionnaire was implemented using Google Forms and made available to government employees from the Smart Zambia Institute (e-Government Division under the Office of the President). Others who participated were from ZICTA, CCPC, IBA, of course the ministry responsible for communications and other statutory bodies, parastatals and the privately owned companies (MNOs and ISPs). Besides, structured interviews were held with ICT experts.

3.2 Research settling

Research settling refers to the place where data was collected from. A non-experimental research design was implemented because the research was conducted in an uncontrolled and natural setting of business life.

For quantitative data collection, random sampling method was used to select respondents from the IT practitioners in the ICT sector to participate in the survey. One questionnaire was used for quantitative data. A non-probability sampling method called purposive sampling was used to identify average citizens to be part of the sample population for qualitative data. Here an average

citizen is one who demonstrated minimum understanding of ICT policy matters especially in e-government. Apart from the Smart Zambia Institute where the questionnaire was distributed to all officers, other organizations starting with the ministry responsible for policy in ICT, regulators in ICT industry and implementing agencies chose one person who answered the questionnaire for qualitative data on behalf of the organization. IT employees and carefully selected ordinary citizens answered the questionnaires in their private capacity as individuals. All respondents were drawn from within Lusaka.

3.3 The Study Population and Sample (The sampling criteria)

Population in this case refers to how many people are there in the group the sample represents. This may be the number of people in a city you are studying. The National ICT policy of 2006 states that given the crosscutting nature of ICT, all line ministries, legislators, traditional leaders, co-operating partners, public sector, private sector, civil society and individuals are key stakeholders to the policy making process. However, with respect to the ICT Portfolio, the Ministry of Communications and Transport is charged with the responsibility of setting the policy direction for the industry and country at large taking into account stakeholder views.

Notwithstanding the above, a four tier system is identified in the ICT sector and the policy tier at national level is made of the cabinet. The tier is as follows; (i) Policy, (ii) Legal and regulatory, (iii) Implementers, and (iv) Consumers.

For this study tier two is referred to as the regulator tier and comprises the main regulator that directly regulates the ICT sector. However, other regulators with a direct or indirect role in the sector were also consider. These were identified as ZICTA, IBA, CCPC and ICTAZ.

Tier three is referred to as the implementer. This tier comprises all ministries and their respective departments, statutory bodies, regulators, parastatals and any other such public institutions that may not have been covered in this description otherwise referred to as MPSAs. (National ICT Policy, 2006)

Tier four comprises the consumers who are the end users of the e-government services, for this population, the research relied on the number of mobile internet users reported by ZICTA survey report of 2018. (ZICTA, 2018)

According to the report, in 2018 the population of Zambia was approximately seventeen million (16, 889,766) of which 18.5% was in Lusaka Province giving slightly above three million (3,124,606.71). The distribution of Internet users across provinces reports Lusaka with the highest percentage at 37% representing a one million plus (1,156,104.48) of the total population in Lusaka (shown with the green marker illustration in Fig. 3.1 below). (ZICTA, 2018)

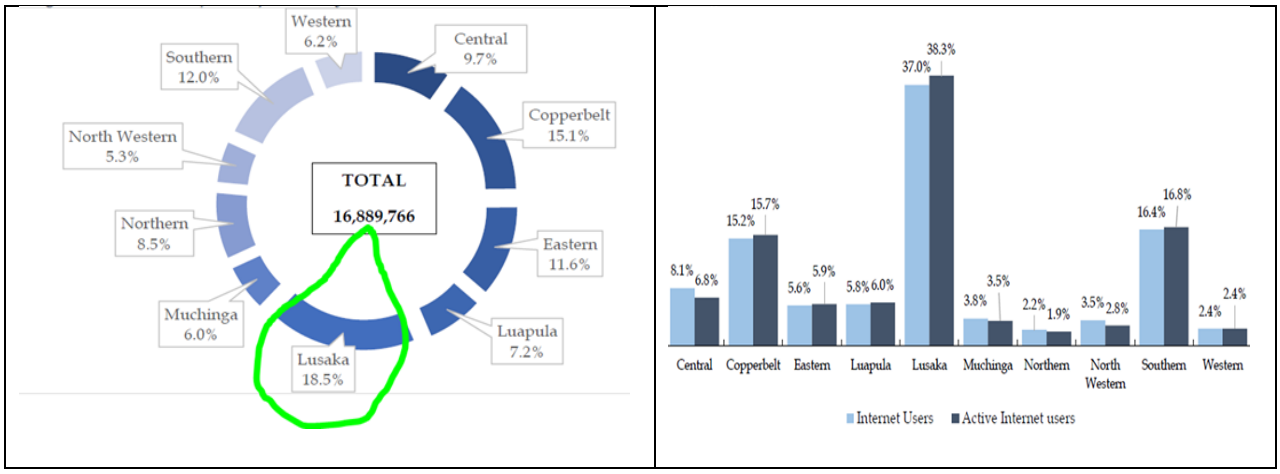

Figure 3.1: National population/provinces and Internet users/province [*ZICTA (2018)*]

Using an online sample size calculator, this population size will require a sample size of about a hundred and two (102) to yield a confidence level of 95% and margin of error of 9.7.

Therefore the sample population was drawn as follows from the four (4) different categories as identified in the 4-tier structure of the ICT sector. (National ICT Policy, 2006)

Table 3.1: Population and Sample size calculation

Tier	**Name**	**Population**	**Sample Size**
1	Policy	2	2
2	Regulator	4	4
3	Implementers	15	15
4	Consumer	81	81
Sampling Frame [Lusaka Province Internet Users]		1,156,105	102
Universe [Zambia]		16,889,766	102

As it was in this study, often one may not know the exact population size. However, the mathematics of probability prove that the size of the population is irrelevant unless the size of the sample exceeds a few percent of the total population you are examining. This means that a sample of five hundred (500) people is equally useful in examining the opinions of a state of fifteen million (15,000,000) as it would a city of a hundred thousand (100,000). For this reason, the Survey System ignores the population size when it is "large" or unknown. (Surveysystem.com) Population size is only likely to be a factor when you work with a relatively small and known group of people for instance the members of an association.

3.4 Instrumentation

The instruments that were used in the collection of data included a self-administered online questionnaire that was also distributed as a hardcopy to some respondents, flash disks, Internet, cell phone, pen notebook and an Internet modem.

3.5 Data Collection (Data Collection instrument, Data Collection procedure)

The collection of data was achieved through self-administered questionnaires, structured interviews, removable disks, Internet, cell phone, pen and notebook:

a) The questionnaire was quite convenient to both the respondents and the researcher
b) The respondents were free to answer the questions at their own convenient time
c) The questionnaire allowed a small amount of time on the part of the researcher and provided consistency in the manner and standard that questions were asked.

The questionnaire was implemented online using the Google Drive Forms facility by Google. The link was shared with carefully selected respondents from public and private sector at various levels of responsibility. Hardcopies were also distributed to some respondents who opted for hardcopy questionnaire and the responses entered into the online system.

Grimm (2010) notes that pretesting is a very important step in survey research as it ensures that all kinds of errors associated with the survey research are reduced. This helped the researcher to see the respondents understood the questions or not while giving an idea on how long each respondent would take to answer the questionnaire. This was achieved by randomly selecting a small number of respondents from the target population and having them to fill in the questionnaire during arranged short sessions. The respondents were able to state which questions were not clear and this helped to improve the quality of the collected data significantly.

Prior to this the questionnaire was submitted to Central Statistical Office (CSO) Statistics Officials who helped valid the data collection tool.

3.6 Ethical Consideration

Resnik et al. (2011) noted that research ethics promote a variety of other important social values such as social responsibility, human rights, compliance with the law and health and safety. In this

study, the fundamental ethical principles were upheld in order to reflect an honest attempt to accurately show the results without being biased. It was also intended to show valuable results that were observed in an ethically conducive and acceptable natural e-government business environment. In this research work it was noted that some of the information received from the respondents was critical to the image of the organizations that they represented and hence the need to maintain confidentiality. The respondents still maintained their right to withhold sensitive or all information if they saw it necessary. Due to the foregoing, the researcher tried as much as possible to respect the views and feelings of the intended respondents when carrying out this study. Many respondents approached to participate in this study expressed their scepticism and discomfort to answer any questions due to what they termed as "sensitive nature" of the area of study or topic. As a result, the researcher never in any way used any form of coercion or undue influence to have the respondents answer the online or hardcopy questionnaire.

3.7 Data Analysis

Google Online Survey Systems has an automated inbuilt mechanism for analysing and interpreting data as the responses are being uploaded online. Thus, quantitative data was analysed using descriptive analysis. A validation mechanism was also activated for questions to ensure the validity of responses, such as ensuring that characters are not entered where number (integers) are expected. In addition, for verification purposes clear presentation spreadsheet (Excel) files were exported from Google Online Survey System. Both applications did make it easier to analyse the various variables and also facilitated the presentation of information in the form of bar charts, pie charts and percentages. The applications were preferred because:

- They are user friendly
- The researcher had some knowledge on how to use the application

- Easy to process and quantify information

On the other hand, the qualitative data was analysed using content analysis approach based on the quantitatively data presented by the online system and the answers from the respondents to the open ended questions in the four different types of questionnaires distributed to the four groups of the IT sector (policy, legal and regulatory, implementer and consumers) .

3.8 Limitation of Study

- Some respondents unnecessarily took long in answering the questionnaire. This delayed the whole process of data collection and analysis.
- Some questionnaires were not completed and some targeted respondents mainly organizations declined participating citing the 'sensitivity of the research topic'. The concern was to give an opinion on the issue of e-government implementation an undertaking of government being coordinated by a division under the Office of the President.
- The research was limited by the fact that some of the terms were unfamiliar in the context used or technical in nature thus posing a communication barrier between the respondent and the researcher.
- Logistical problems were also encountered as respondents though within Lusaka city are not found in one locality in proximity to one another, this entailed several errands to and from while distributing and collecting the questionnaires.

3.9 Chapter Summary

This chapter dealt with the methods that were employed in the collection of data. The research used a mixed method approach in order to get the benefit of both the qualitative and quantitative design. It showed how the methodology used would address the issues raised in the research

questions. It further highlighted the instruments that were used during the data collection and also reviewed some of the limitations that were encountered during the process.

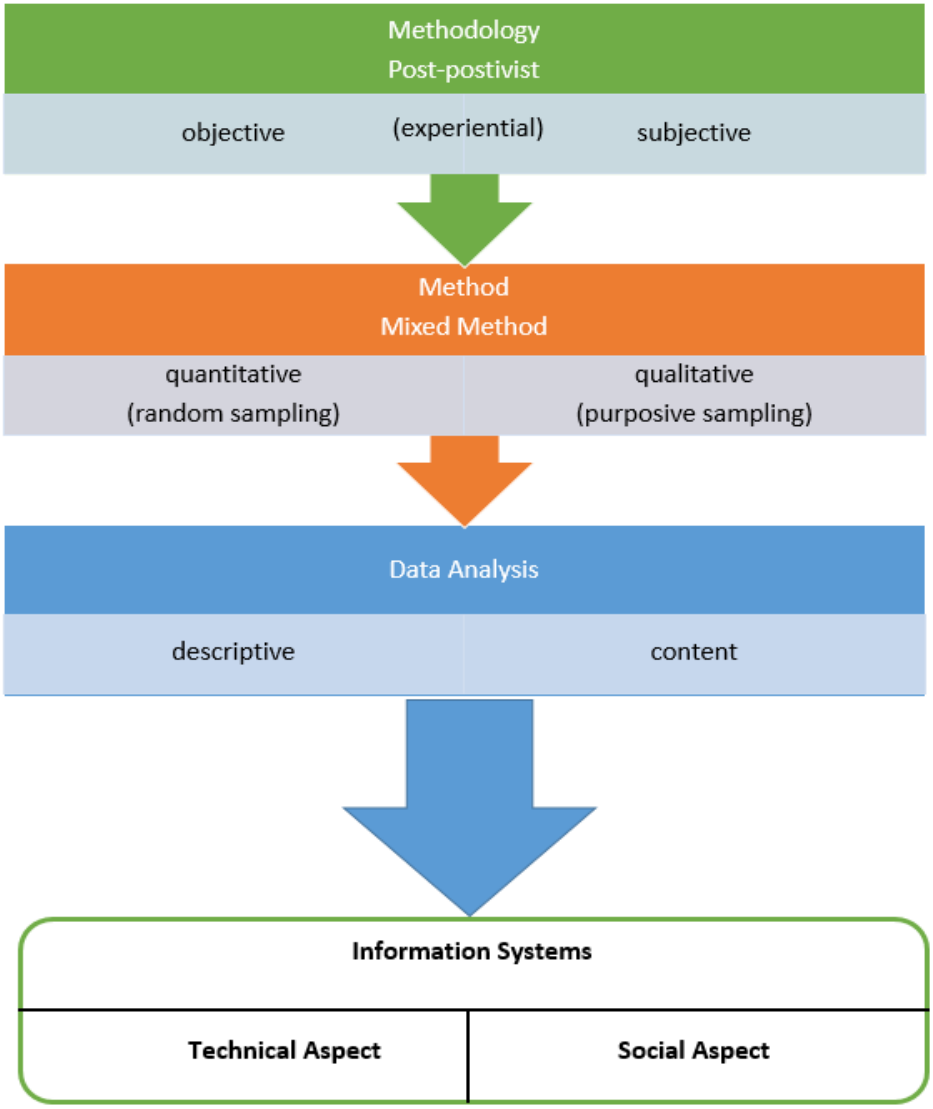

Fig 3.2: Summary of the research design

CHAPTER 4

4.0 Results

In this study, the Google online questionnaire was administered alongside hardcopies to some respondents who preferred the hardcopy questionnaire (See Appendix I). All the hardcopy questionnaire responses from quantitative data collection were manually entered into the system by the researcher. The embedded automated data analysis system in Google Drive/Forms automatically generated the graphs and tables that were used for data analysis. The tool was found to be very convenient to administer the questionnaire to some respondents as they could do it in their on time. Other respondents were also given the option of the hard copy questionnaire.

The online Google Survey System has a web interface for both the design and respondent side with a simple and interactive page layout making it very user friendly. The system automatically generates the statistical graphs and tables which can easily be copied to the report. The researcher also had the option of exporting the data collected into a spreadsheet that can further be used in other data analysis tools such as Statistical Package for Social Scientists (SPSS). The following are the results;

The demographic findings as shown in table 4.1 below, revealed that seventy-eight (78) were male representing seventy-six point nine (76.9%) of the total while the female were twenty-four (24) representing twenty-three point one (23.1%) of the participants.

4.1 Demographics of the study

Table 4.1: Gender distribution of respondents

Gender	Frequency	Percentage
Male	78	76.9
Female	24	23.1
Total	**102**	**100**

Those who are married accounted for ninety-two point three (92.3%) while seven point seven (7.7%) are single.

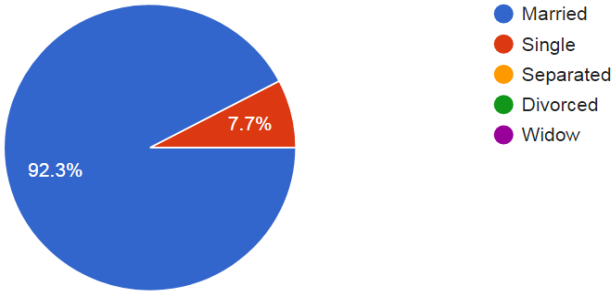

Fig 4.1: Marital status of respondents

It is also worth noting that the same 92.3% accounted for respondents with families while 7.7% had no families. The oldest respondent was sixty (60) years of age while the youngest was twenty-five (25) years old. The majority of the respondents were fifty (50) to fifty-six (56) years of age at fifteen point four (15.4%).

The majority of the respondents were Christians at over ninety (92%) while eight (8%) accounted for other religions. This statistics is also true for ethnicity as well. In addition, the figure below also shows the educational background of the respondents. Similarly, the majority at 92.3% are university degree holders while 7.7% are college diploma holders.

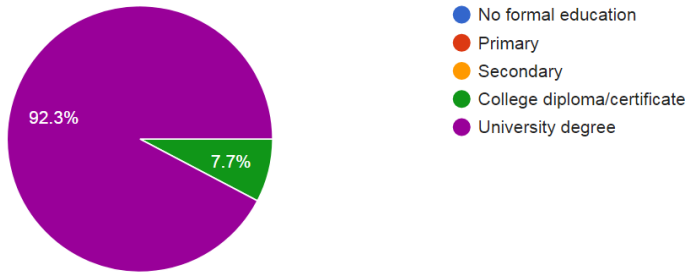

Fig 4.2: Formal training of respondents

The areas of specialization for the respondents in the upper three tiers of the ICT industry, that is, the policy, regulation and implementation were captured as follows; forty-six point two (46.2%) Computer science/IT, thirty point eight (30.8%) Engineering, Economics and Business/Accounting were seven point seven (7.7%) each and other specialties fell in the remaining 7.7%.

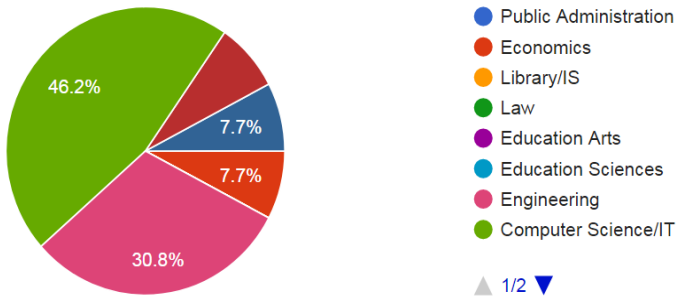

Fig 4.3: Areas of study of respondents (1 of 2)

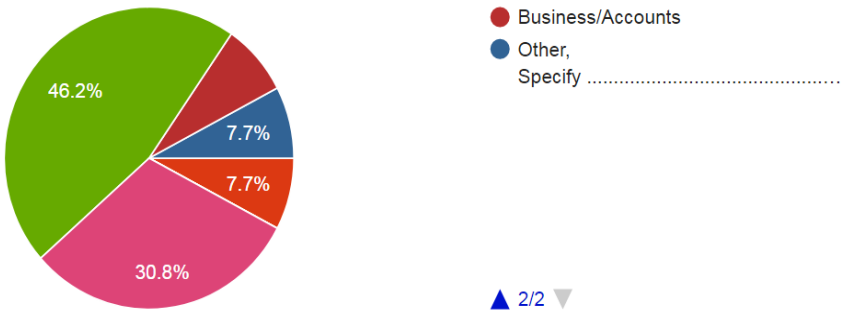

Fig 4.4: Areas of study of respondents (2 of 2)

The classification of roles for the respondents was as follows;

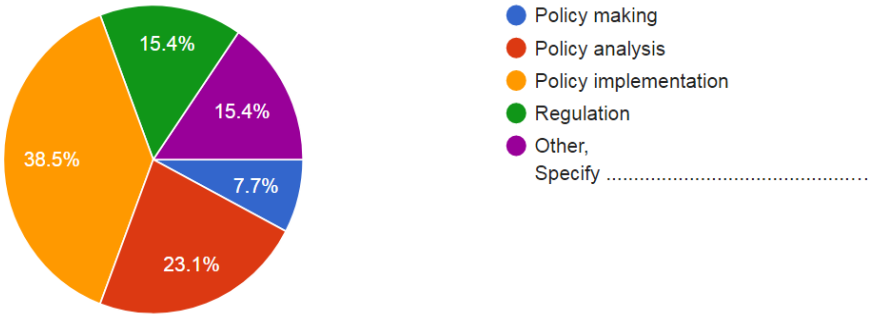

Fig 4.5: Classification of roles

The highest was in policy implementation at thirty-eight point five (38.5%) while the lowest was seven point seven (7.7%) for policy making.

The study has revealed that the major hindering factors to e-government implementation in Zambia are;

i. Infrastructure
ii. Citizen ICT literacy levels
iii. Policy vacuums and political will and
iv. Funding

4.2 E-Government policies, adoption and deployment

The study revealed that Zambia has policies that guide the adoption and deployment of e-government at national level. The history of these polices can all be traced to the first government document that address ICT matters, this is the National ICT Policy 2006. This policy states that; at the national level, the importance of ICT in national development is demonstrated by the approval of the ICT Policy and the inclusion of ICT as a priority sector in the Fifth National Development Plan 2006-2010. This Policy is designed on twelve pillars (among them is e-government security in information society and ICT services) as follows:-

1) Human Resource Development
2) Agriculture
3) Tourism, Environment & Natural Resources
4) Education
5) Health
6) E-Commerce
7) E-Government
8) Youth and Women
9) Legal & Regulatory Framework
10) Security in Information Society
11) Access, Media, Content and Culture
12) ICT Services

The policy also structures the ICT sector as sector represented by a four-tier system, namely policymaking, legal and regulatory framework, operators and consumers (end users). This is a framework adopted to classify respondents in this study as well but focuses mainly on the G2C

and G2E interactions of e-government as earlier shown in the proposed theoretical framework (The G2C/G2E Matrix). Each of these tiers play a unique role in e-government implementation.

Mzyece (2012) notes that in this policy, ICTs are presented as the means of e-government, while electronic interactions and transactions are regarded as primary in delivering public services and in promoting e-government.

He further notes that good governance has been identified as a cross-cutting issue in the fifth and sixth national development plans. E-governance has been identified as a powerful enabler of good governance and e-governance programmes are explicitly defined and budgeted for in all the subsequent national development plans. E-government is regarded as a national priority and therefore deserves attention from scholars and policymakers interested in the development of e-government in Zambia. However, the reality of e-government progress has fallen far short of its potential and its stated importance in policy documents.

The study reviewed that the incorporation of ethical issues in e-government implementation is relevant. Half (50%) of the respondents feel that ethical issues are very relevant.

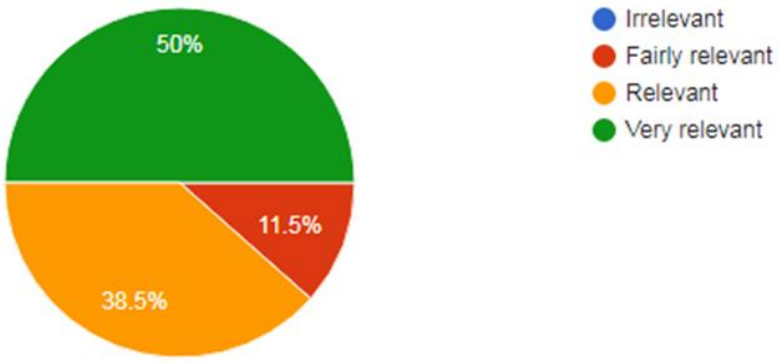

Fig 4.6: Relevancy of ethical issues to e-government implementation

It was also found that over forty (44.4%) of the respondents are not sure if the Zambian e-government policy addresses ethical issues that arise in e-government implementation. Only

thirty-seven 37% affirmatively say that the policies addresses the ethical issues and eighteen point five (18.5%) disagree.

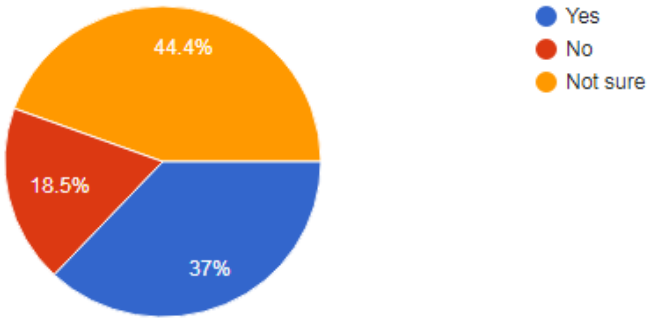

Fig 4.7: Does e-government policy address ethical issues

The legal and regulatory framework is established by the following pieces of legislations;

(i) ICT Act 2009

(ii) ECT Act 2009

(iii) IBA Act 2002 and the

(iv) ICTAZ Act 2018

The other e-government policy documents from the National ICT Policy is the now implementation document called the SMART Zambia Master Plan 2016 – 2020. The Master Plan states that the scope of the e-Government Projects is holistically divided into broad phases of five years each. The initial five years are very important for laying a solid impeccable foundation for the development and sustenance of e-Government in Zambia. Therefore phase one (2016 – 2020) will be focused on the fundamental ICT pillars which according to the Beuchuma Model include the governance infrastructure, technical infrastructure and the knowledge infrastructure for the ICT Infrastructure.

The same document however indicates that at the beginning of the implementation of this master plan Zambia is said to be between web presence and interaction (which is low) in the e-Government Maturity Model (See figure 2.9).

This study has revealed that ethical issues are very relevant to the implementation of e-government yet over half (53.8%) of the respondents fairly agree that the e-government implementation policies address these ethical issues.

Further, the study also revealed that fifteen point four (15.4%) of the respondents feel that the current ICT policies adequately address the ethical issues that arise in e-government (other than e-government policies, bills and acts). Over half (53.8%) only fairly agree so. 7.7% strong agree while twenty-three point one 7.7% disagree.

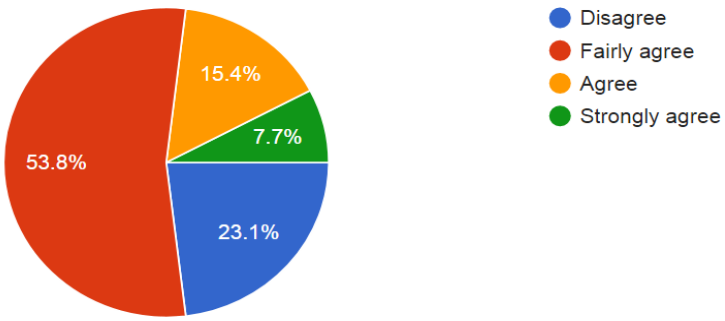

Fig 4.8: Do other laws address ethical issues?

4.3 Ethical issues in e-government implementation

The study revealed that over half (53.8%) agree that ethical issues are very relevant to e-government implementation while slightly above thirty (30.8%) agree they are relevant. Fifteen point four (15.4%) say they fairly relevant and none responded that ethical issues are irrelevant.

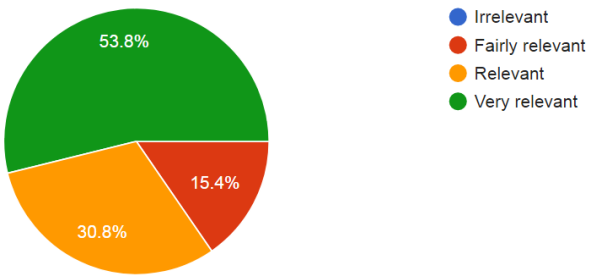

Fig 4.9: The relevance of ethical issues to e-government

Stahl et al (2016) notes that only with a clear understanding of the social and ethical issues can these be proactively addressed, that is, be anticipated, reflected upon, deliberated with the public and other stakeholders, and be responded to.

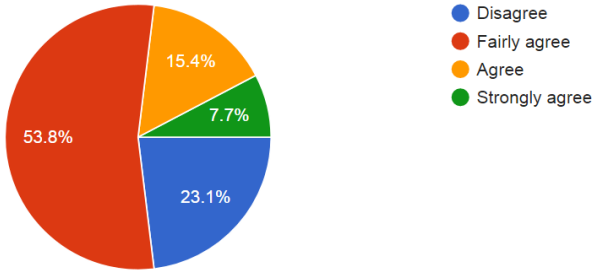

Fig 4.10: Do current ICT policies adequately address ethical issues?

Over twenty (23.1%) of the respondents feel that the current ICT policies (other than the e-government policies, bills, and acts) do not adequately address ethical issues that arise in e-government implementation. Over half (53.8%) only fairly agree so and only slightly above fifteen (15%) agree so with 7.7% strongly agreeing so.

As early as the National ICT Policy of 2006, the Zambian government noted among the goals of the policy that the emerging trend for increased information access/exchange resulting from integrating ICTs within the social, cultural and economic sphere of the country also brings to the

fore a number of security, privacy and consumer protection issues that need to be addressed as part of the efforts of developing an information society. It is noted in the policy that Zambia like most countries in the world is vulnerable to some of the negative implications that may hinder the mainstreaming of ICTs in society. Therefore, specific security measures and mechanisms to ensure the safety of citizens, communities, businesses and the nation at large are needed as part of implementing the policy.

The study also shows that ethical issues are not immediately associated with successful implementation of e-government. Infrastructure is identified by close to forty (40%) of the respondents as the major challenge to e-government implementation in Zambia. This is followed by citizen literacy at over twenty (23.1%). The others are policy and political will both at fifteen point four (15.4%) and the least is funding at close to eight (7.7%). Bwalya (2009) notes that lack of adequate ICT infrastructure and political will, provision of content in English other than local languages, lack of proper change management procedures, non-contextualization of e-government practices are among the major factors that contribute much to the delay in appropriate e-government adoption in Zambia.

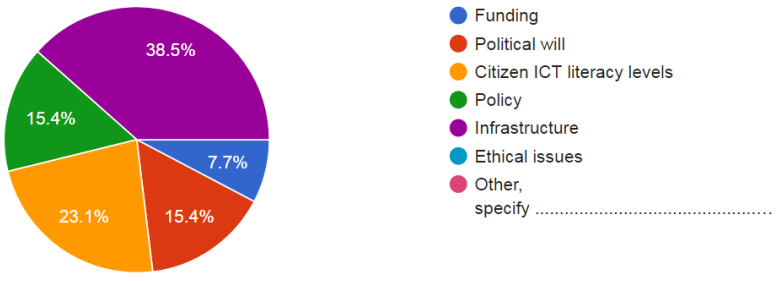

Fig 4.11: The major challenges of e-government implementation in Zambia

However when probed further, the users show a great appreciation that the inclusion of ethical issues in the designing of information systems for e-government will increase citizens' embracing and adoption of e-government.

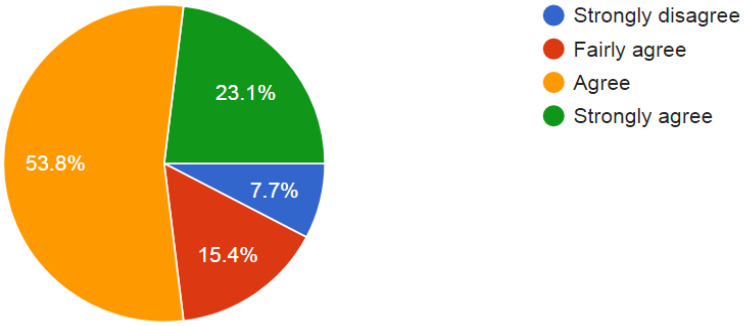

Fig 4.12: Addressing ethical issues will increase citizens' embracing e-government

As shown, over half 53.8% agree while twenty-three point one (23.1%) strongly agree that the inclusion of ethical issues in e-government implementation will increase citizens/businesses embracing of e-government.

Table 4.2: The most prominent ethical issues in e-government

Mention any five (5) of the ethical issues in the e-government policy	Responses	
	N	Percent
Security	25	24.8
Privacy	21	20.5
Universal access	9	8.7
Good governance, Trust	13	12.6
Confidentiality, integrity, accountability	17	16.6
Fairness	7	6.8
TOTAL	102	100

The study shows that the most prominent ethical issue is security followed by privacy at slightly over twenty-four percent (24.8%) and 20.5% respectively as shown in Table 4.2 above.

4.4 Policies, mechanisms and systems addressing ethical issues

The study also revealed that when addressing the ethical issues that arise in e-government, policy framework formulation should precede systems design. According to the study, over half (53.8%) of the respondents agree that the designing of information systems is preceded by formulation of a policy framework that addresses the ethical issues. The respondents also affirmatively agree that systems can be designed in such a way that they can address the ethical issues identified.

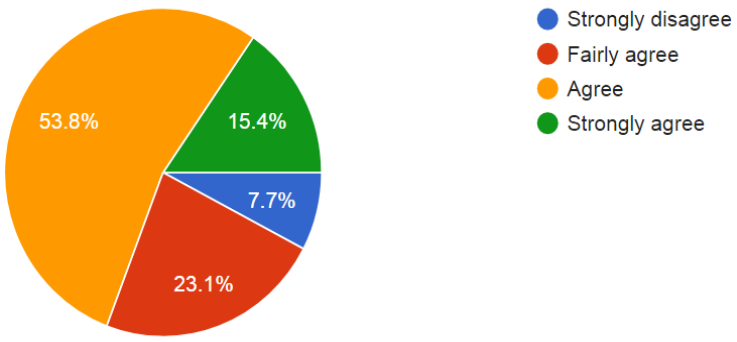

Fig 4.13: Policy framework precedes systems design

4.5 The role of professional regulation in addressing ethical issues in e-government

The study revealed that the regulation of professionals will help increase the confidence and trust in information systems designed for e-government among the end users. Over sixty (60%) overwhelmingly agree so with thirty-eight point five 38.5% strongly agreeing. Thirty (30.8%) fairly agree.

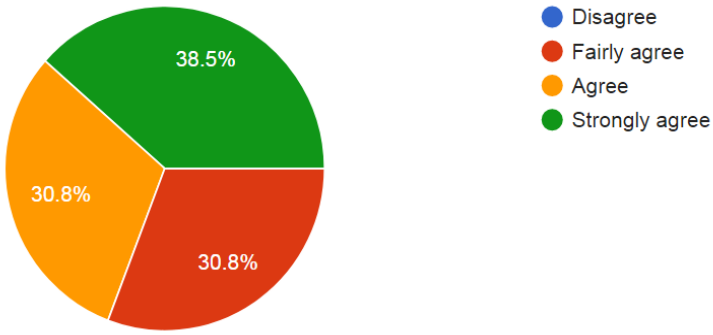

Fig 4.14: Professional regulation will increase the confidence and trust in e-services

From literature reviewed, results point to the fact that computing is now considered a profession. (Loui and Miller, 2008) According to Laudon (2008), when groups of people claim to be professionals, they take on special rights and obligations because of their special claims to knowledge, wisdom, and respect. Among other things, this is achieved through one of the five characteristics of a profession, that is, the control of the professional practice by other professionals. This option is called self-regulation while professions regulated by governments are said to be under direct regulation. In addition professional regulation entails the establishment of a professional code of conduct. A professional code of conduct for IT government employees will work to ensure that the professionals with access to personal and government information will always act responsibly and put the interests of the citizens and the governments respectively first.

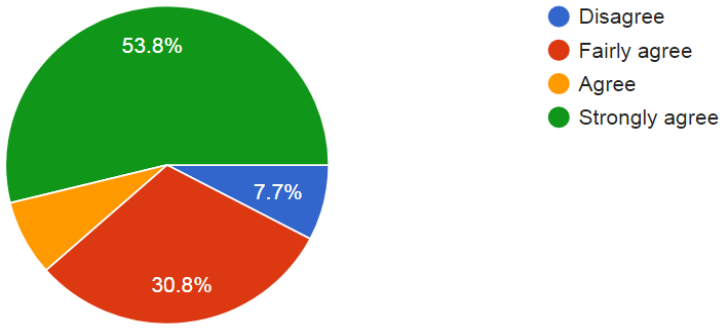

Fig 4.15: Professional regulation help achieve realization of professional values

The study also revealed that professional regulation will help in the realization of professional values;

- Commitment
- Responsibility
- Integrity and
- Accountability

Among IT professionals. According to Kizza (2007) these are the cornerstones of professionalism. It has also shown that over ninety (90%) agree that regulation will help improve public perception of the IT professional thereby increasing trust in the electronic services.

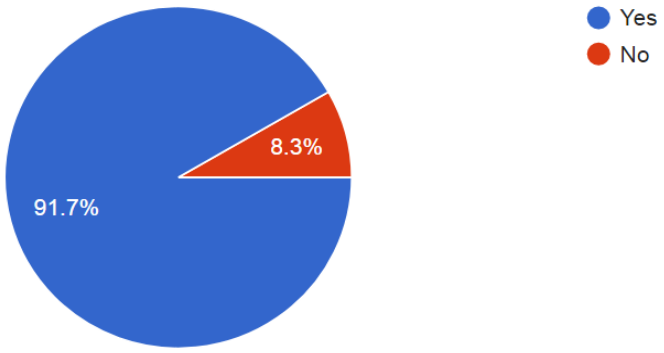

Fig 4.16: Will regulation improve public perception

Put in other words, with regulation in place, the public gets to be assured that the IT professionals are being kept in check and made to conform to a code of ethics. This gives the citizens the assurance the professionals will not abuse their privilege of access to individuals' private information and use it for other motives.

4.6 Results validation

By virtue of using the mixed method approach (quantitative and qualitative data collection methods) the results collected were cross-validated as the structured interviews held with some experts provided an opportunity to understand and confirm the quantitative data collected through the questionnaire. A triangulation approach was also tenable to validate the data as the participants in the study were drawn from the four tiers of the ICT industry as outlined in Table 3.1.

4. 7 Significance of the statistics in this study

The significance of the statistics in the study is as follows;

i. The statistics indicates which of the ethical issue is ranked as a major issue in e-government implementation.
ii. The statistics also brings out data as to how much knowledgeable the IT experts are with IT policies in the country
iii. Over and above, the statistics also indicate how the respondents feel ethical issues are relevant to the implementation of e-government.

4.8 Chapter Summary

A total of one hundred and fifteen (115) responses both electronic and hardcopy were received. Only one hundred and two (102) were validated for this study in line with the sample size calculated. Of the 102 received questionnaires, seventy-eight (78) were male while twenty-four (24) were female respondents and represented close to seventy-seven (76.9%) and over twenty (23.1%) respectively of the sample. It was noted from the study that ethical issues have an impact on e-government implementation, the most prominent ethical concerns are security and

privacy and that the design of systems to address these ethical issues is tenable and should be adopted to address the concerns and thus increase trust and confidence in the public (G2C) for successful implementation of e-government. In addition, in systems design and analysis policy precedes design and also professional regulation addresses ethical issues among government employees (G2E) and also has a positive impact in the citizens' trust in the e-services deployed for e-government implementation.

CHAPTER 5

5.0 Discussions and Recommendations

5.1 Discussions

In conclusion, ethical issues have a major impact on the successful implementation of e-government in all societies, developed or developing. The most prominent of all the ethical concerns being cyber security and data privacy. Though not identified by policy makers in developing countries, for instance the Case of Zambia, if not factored in the development process, the omission of ethical issues will result in the design and deployment of electronic services that will be shunned by the users thereby resulting in low adoption of the e-services; this will in turn result in e-government failure. Due to the fact that ethical issues (phronesis) are not identified as a major factor in e-government implementation, it goes without saying therefore that, little or no funding is allocated to address the ethical concerns as compared for instance to infrastructure (techne) development. In the case where ethical issues are tackled, it is done out of context of ethical concerns and each ethical issue is addressed in isolation resulting in policy silos, incoherencies and inconsistencies.

The literature reviewed show that systems can be designed in such a way as to address the ethical concerns that arise in the use of information technology. This is referred to as Value Sensitive Design (VSD). However, this should be preceded by policy design. The policy serves as a framework that will provide guidelines for the process of identification of ethical concerns and mechanisms for addressing the concerns including the design of systems that take into account the ethical concerns. The literature further reveal that professional regulation will also help address the ethical issues that arise in the G2E interaction of e-government by enhancing

professionalism among the IT professionals working in e-government delivery thereby increasing trust and confidence among citizens.

5.1.1 Ethical Issues in e-Government Implementation

Ethical issues have an impact on e-government undertaking, therefore there is need to factor in the implications that these ethical issues have on e-government adoption and deployment to ensure the successful implementation. The inclusion of which must be right from the onset, that is, from policy planning level through to systems implementation, will increase the confidence of citizens in the use of e-services as the end users. The survey results showed that the widely accepted major challenges to e-government implementation are infrastructure, citizen ICT literacy levels, policy, political will and funding in that descending order. Ethical issues are not identified as a major challenge. Therefore, it is easier to conclude that these are the areas that are prioritized and receive more attention in terms of funding and implementation programmes.

The most prominent ethical issues identified by many users are security and privacy. In short the major concern by many users as well as the designers of e-government are the security of both the systems and the personal information these systems will store and transmit. There is low awareness among citizens that the Zambian E-Government Policy and other ICT policies do address some ethical issues that arise in e-government implementation, however, the obvious fact is that these policies do not adequately address all the ethical issues that arise and accord them the attention they deserve. In addition, where the ethical issues are addressed they are addressed out of context of ethical issues and the formulation of these policies is in silos. For instance, the process of formulating a policy tackling security does not take on board concerns about intellectual property, hence the existence of two policies or laws that do not talk to each other

(The ZAMCOP Act and the proposed Cyber Security Bill). In the same vain, while tackling national security the privacy of citizens may be violated.

The major ethical issues identified by the users are not properly defined in these policy documents and clearly differentiated for the purposes of understanding their unique and/or common attributes and interrelationships. The ethical issues that arise in e-government implementation as established in this study are; privacy, confidentiality, computer crime (cybercrime), computer decisions, technological dependence, reliability, integrity, security, intellectual property, anonymity, legitimacy, internet addiction, computer technology for persons with disability, digital divide, trust, fairness and good governance. This list may not be exhaustive. The G2C/G2E Matrix can be used as discussed in section 5.2.1.

5.1.2 Impact of Ethical Issues on e-Government

According to the study, ethical issues have an impact on e-government. This means that the levels of awareness of different types of dangers of the internet risk have a direct bearing on the adoption of e-commerce by users of internet services. This impact of the ethical issues is on both sides of e-government, G2C and G2E but probably in directions. The failure of coding algorithms correctly on the G2E will result in a service with adverse results to the users on the G2C. (The bank loan algorithm). The addressing of ethical issues in e-government implementation increases citizens/businesses embracing of e-government. Further, the study revealed that the impact of ethical issues in e-government implementation is not instantly recognized by both the users and implementers (in their ranks and file, from policy to system design). Hence, ethical issues are not mentioned as one of the major challenges to e-government implementation. Policy makers do not possess detailed knowledge about ethical issues. The

concepts and theories about the subject still elude their collective perception and judgment about their impact on e-government implementation.

The impact of the ethical issues on the consumers is seen as they make decisions on how information systems address their moral concerns such personal information privacy, system reliability, system availability. The other ethical concern that impacts the acceptance and subsequent adoption of e-services deployed in e-government is the systems inbuilt tendency to promote or demote certain values in society. For instance, the concern that information technology will increase government's ability to conduct surveillance on its citizens. The third concern with even greater impact on e-government boarders on government employees themselves. The question that is posed is, will the IT experts who by virtue of their positions have access to so much information (about citizens and government) and powerful tools at their disposal remain professional to safeguard the interests of both the end users and the establishment? For example, will the IT employee respect an order from the superiors to have back-end access to encrypted messages belonging to a private citizen when the citizen was assured when registering to use the system that their messages are end to end encrypted and no third party can have access to them including government? The fourth concern in the quadrant is the assurance governments will practice good governance and be accountable to its citizens thereby putting in place all mechanisms to address the concerns. This will increase the trust in citizens which will result in increased confidence in the adoption of the e-services.

5.1.3 Policies and Mechanisms

From the above conclusions, it becomes very vivid therefore that the successful implementation of e-government will mainly depend to how the policy dimension is capacitated to understand

the underlying implications of information technology and how policies can be translated into systems that are able to address all requirements outlined at policy level, including the ethical effects of these artefacts. In conclusion therefore, policy is the beginning of everything when it comes to resolving the ethical issues that arise in e-government implementation. It is the bedrock that provides a framework upon which all mechanisms and processes within the organization to address the ethical issues are based. Policy will also provide the overarching guidelines and detailed procedures for the design and deployment of systems that address the identified ethical issues. The submission by majority respondents that they are not sure the e-government policy addresses ethical issues might stem from the fact that the SMART Zambia – e-Government Master Plan, which is the guiding policy implementation document, does not directly and comprehensively tackle ethical issues. The only ethical issues mentioned in the National ICT Policy are security and privacy. Although the National ICT Policy clearly structures the ICT Sector by clearly outlining the four tiers that make up the sector, it does not go in detail to identify the ethical issues that will arise as the nation embarks on the transformative journey of e-government and recommend strategies that will be used to address them. By their very nature, ethical issues are multi faced, interrelated and therefore multi sectorial. That is, they cut across a number of sectors in the political, social, cultural and economic spheres of our society.

Other than e-government policy, other ICT policies do address some of the ethical issues identified, these are mainly security and privacy in the ICT and ECT Acts of Parliament. Despite the fact that these laws have been in existence for 10 years now, citizens still feel that security and privacy remain a major concern. The conclusion of the researcher is that this is because both security and privacy are not being handled as ethical issues but rather as infrastructure. This

therefore means that solutions devised to address the concerns are inappropriate for the problem at hand.

It is also safe to conclude that there exists 'policy vacuums' in as far as the comprehensive addressing of ethical issues in the Zambian E-government implementation agenda is concerned. These policy vacuums stem from the fact that policy makers and analysts only possess a fair knowledge (slightly below average as results of study show) of ethical issues that arise in e-government implementation in developing countries such as Zambia according to the study. This fair knowledge also extends to the understanding of the underlying concepts and theories of ethical issues in the introduction of ICT tools for management in government and public service delivery. Consequently, the right perspective incorporation of ethical issues in e-government as demonstrated in this study continues to suffer.

5.1.4 Information Systems that address Ethical Issues in e-Government

Information systems can be designed in such a way as to address the ethical concerns that arise in their use the study revealed. Just as technological artefacts can promote the realization of values, they can also promote the enforcement of norms. Embedded norms are a special kind of built-in consequence. They are tendencies to effectuate norms by bringing it about that the environment behaves or is organized according to the norm. For example, web browsers can be set not to accept cookies from websites, thereby enforcing the norm that websites should not collect information about their user. By enforcing a norm, artefacts thereby also promote the corresponding value, if any, for instance, privacy in the example. (Floridi, 2010). The PDE model discussed in Section 2.6 is in tandem with the findings of this study where overwhelmingly 92.3% of the respondents agree that policy develop must precede any systems

design. Therefore a policy that does not include ethical issues at the beginning will result in design that is not sensitive to the human values and thereby posing adverse effects when the designed products are now in use.

5.1.5 The Role of Professional Regulation

From the study, it can be concluded that professional regulation can contribute to the building of trust and confidence of the citizens as they interact with government e-services assured that the government employees empowered to be custodians of the systems and personal information have a code of conduct that compels them to be professional and ethical to avoid abusing their privilege. The study shows that IT professionals have a major role to play in addressing ethical issues that arise in e-government implementation. As they develop policy, design systems and use the systems to provide a service to the citizens, the employees' interactions with the 'systems' in place, be it manual or computer based, within government agencies is referred to as G2E interactions. The study shows that the citizens expect the government employees to uphold all the following professional roles;

i. Commitment
ii. Responsibility
iii. Integrity, and
iv. Accountability

The above four are the pillars of professional regulation. (Kizza, p70) In addressing ethical issues that arise in e-government, some measures will not include the designing of computer based systems. For instance professionalism. This is a specialized area of study beyond this research, notwithstanding, this study can only go as far as concluding that the introduction of professional regulation as shown in the study will significantly increase e-government success. Many studies

on the ethical issues that arise in the introduction of information technology by computer experts for that matter have made reference to this subject matter.

Other than IT, non IT employees also form part of this governance dimension (Fig 2.2). Little prominence is given to the non IT back office (government employees) that will be affected by the implementation of e-government due to the reforms in business processes, standard operating procedures and workflow relationships, this study also only picked on the IT employees. This need not be the case, because in the public sector, just like in the private sector, any organization that undergoes the four kinds of structural organizational changes which are enabled by information technology, these are, automation, rationalization, reengineering and paradigm shift all employees are affected. The third phase called reengineering heavily affects these non IT back office (government employees) as it involves reforming processes, standard operation procedures and workflow relationships. It is not uncommon, and often than not, it is the case to associate human capacity in terms of citizen's knowledge of ICTs with the failures of e-government implementation than to the non IT employees of government's failure to adapt to the changes brought about by information technology.

In addition, it is very unusual to relate any e-government implementation failure, or indeed, any IT project to lack of full knowledge of the ethical issues introduced by the IT systems by the policy makers and the IT professionals. Let alone the ethical issues that arise in the implementation of ICTs for public service delivery in government on both government employee side and citizens as users. There are ethical issues that arise in both the governance and outreach dimensions of e-government that need to be factored in the policy dimension. Professionalism should cater for both IT and non IT employees for the G2E to be water tight. However, this study emphasizes the professionalism of the government IT employees only.

5.2 Recommendations

5.2.1 Identification of ethical issues in e-government

Due to their similar nature (ethical issues arise because humans are moral beings and engage their moral intellect to make moral decisions), it is recommended that all the ethical issues that arise in the introduction of information and communication technologies in government for management and public service delivery should be identified and the e-government interaction (G2C/G2E) they affect. The G2C/G2E Matrix developed in this study (Figure 1.6) can be used to identify the interaction(s) where each ethical issue arise thereby isolating ethical issues to either be G2C or G2E oriented or both so that appropriate policies could be designed to address them and further serve as a framework that will guide the development of mechanisms and computer based information systems that take into account the ethical concerns. Mechanisms are to be understood as business processes and operating procedures put in place and some of which are followed organization wide by all employees to provide services to citizens while other are followed in the design of information systems by IT experts and subsequently in the usage of the developed systems as they provide a service to citizens and by the citizens themselves.

In addition, a complete identification of all the ethical issues that arise in both interactions will also help how they are classified based on the evaluation of the extent to which the types of moral wrongdoing are related specifically to the technologies used. (Such as Determined, Related, Dependent and Specific) electronic environment as discussed in Section 2.4.

Further studies could be done to understand if ethical issues have generic characteristics that can be analysed in detail together. A classification of e-government ethics by Ramadhan et al (2011)

who postulated that there are three applied ethics, in the world of computers science, that is, computer ethics, information ethics, and cyber ethics is recommended as shown in Section 2.4.

5.2.2 Understanding the impact of ethical issues on e-government implementation

It is recommended that each of the ethical issues must be defined and explained in detail and their impact explained in full.

Horner and Mullen (2004) note that in essence, the ethical situations in which computers, digital technology and electronic environments are involved do not require a totally innovative ethical approach. Similarly the steps needed to address the varieties of moral wrong doing in electronic environments may already be part of existing policies for the regulation of the business environment or in promoting ethical cultures and corporate responsibility. Therefore, the separation of the impact of ethical issues and how their impact is exacerbated by computer technology should be understood to ensure the correct solutions are developed.

Further to reduce on the impact the ethical issues can have on e-government success it is recommended that the change management process in e-government should take on board ethical issues study. One thing ignored is that e-government is not an end in itself but a means (tool) to an end. Being a tool to improve service delivery in the public sector, the tool must not therefore prove to be an impediment to the achievement to the objectives.

5.2.3 Policy formulation precedes Systems Design

As established from the results of this study, it is recommended that the formulation of policies in e-government must precede any system design using the PDE model discussed in Section 2.6. This is in conformity with results of this study that the designing of information systems that address ethical issues is preceded by a policy framework that addresses ethical issues.

It is therefore recommended that this process is followed iteratively until the desired effects of the IT artefacts is manifested as aspired in the policy.

As noted by Horner and Mullen the field of Computer Ethics provides valuable approaches to the 'policy vacuums' created by the ubiquity of ICTs. Therefore it is recommended that computer ethics is considered a valuable tool in resolving the ethical issues that arise in the use of all computer technology even in this case of e-government implementation in Zambia. The design of systems should not be left to the choice and test of the ICT specialists but rather be a reflection or implementation of the solutions to the identified ethical issues that arise in the use of the IT artefact being designed to be deployed for public service in e-government.

Ethical issues are multifaceted and cross cutting, it is required that a multi sectoral approach is adopted to deal with them. This is so because as earlier noted some of the ethical problems not necessarily be specific, determined or dependent on electronic environment but only related to it. This means that these ethical concerns also exist in other realms of society and not only in the use of ICT.

Below is a table developed and recommended by the author that can be used in depicting ethical issues identified from both G2C/G2E interactions, stipulated policies and System design mechanisms to address the ethical concerns that arise in e-government implementation. The solution process for each ethical issue starts from the left to right there after following the Policy – to – Design – to – Effects (PDE) Model to translate the policy into a system design solution that addresses the identified ethical issue.

Table 5.1 Ethical issues identification, Policy and System design

	Ethical Issue	Policy	Internal/ External	Process/System Design
1.	**Security**	ICT, ECT, Cyber Security Act, Organizational ICT Policies	G2E/G2C	User profiles/Accounts, Passwords, Antivirus, ACLs, Port Security, Firewalls, DMZ, Biometric Access Control, Firewalls, Intrusion Prevention Systems, Basic User training
2.	**Privacy**	GDPR (domestication), other local legislation	G2E/G2C	Data encryption, Biometric, Passwords, User Accounts/Profiles, Firewalls, Intrusion Prevention Systems, Basic User training
3.	**Intellectual Property (IP)**	ZAMCORP Act, Patents/Copyright Acts	G2E/G2C	Hologram, Patents/Copyright Registration Certificates, Counterfeit detection systems
4.	**Computer Technology for People living with disabilities**	UAS	G2E/G2C	Computer keyboard braille, Text-to-speech accessibility tools,
5.	**Trust**	IEC/FCC/ZABS/ZICTA/	G2C	Standard/ Authenticity certificate
6.	**Accountability**	Professionalism,	G2E	Audit trails/System audits, ISACA/CISA
7	**Reliability**	QA	G2C/G2E	System backup off site, SDLC, Best practices in Project Mgt (PRINCE2)
8.	**Fairness**	Professional bodies ICTAZ, EIZ	G2E	Code of Ethics
9.	**Good governance/legitimacy**		G2E	COBIT 5 etc.
10.	**Digital divide**	UAS Policy	G2E/G2C	USF, User training
11.	**Internet addiction**	Organizational ICT policy	G2E	Content filtering (Checkpoint, Proxy server),

5.2.4 Value Sensitive Design (VSD)

This current study has established that, it is very possible to design systems that address the ethical issues that arise in e-government implementation. Therefore, the approach called Value Sensitive Design is recommended as the approach that should be adopted in all e-government systems development. Value Sensitive Design is a theoretically grounded approach to the design of technology that accounts for human values in a principled and comprehensive manner

throughout the design process. It employs an integrative and iterative tripartite methodology, consisting of conceptual, empirical, and technical investigations. (Friedman et al in Himma and Tavani, 2008) In addition to the operational definition given in Chapter One, value in this context refers to what a person or group of people consider important in life.

In today's world we act through information technology (IT), are restrained by it, use it to influence people, to express ourselves, and so on. IT has an enormous impact on our (moral) lives. IT is a generic notion that encompasses many things from computers, the components that computers are made of, the software that runs on the computers to hard disks. As these IT-artefacts become more and more sophisticated and embedded in our lives the question arises what the moral status is of these IT artefacts. That they do have moral impact seems self-evident but can they be said to act morally?

In the 1950s, during the early periods of computerization, cyberneticist Wiener (1953, 1985) argued that technology could help make us better human beings and create a more just society. But for it to do so, he argued, we have to take control of the technology. With the coming of Artificial Intelligence (AI) this subject has become even more important in our information society (e-society). Although IT is a generic notion that can encompass many things from computers and the components that computers are made of, to the software that runs on the computers, from configuration management tools to avatars, from databases to HTML pages, the approach of VSD should become the de facto standard in Systems Analysis and Design so that all IT artefacts exhibit all ethical concerns that may arise as a result of their use. Whereas a few decades in the past IT artefacts were considered morally neutral, with the advent of AI, it is possible to do an ethical study of computer systems themselves independently of their use by human beings, ethics of computer systems separate from the ethics of using computer systems.

It is therefore recommended that for e-government the embedded values approach in computer ethics, formulated initially by Helen Nissenbaum (1998; Flanagan, Howe and Nissenbaum 2008) should be adopted. The embedded values approach holds that computer systems and software are not morally neutral and that it is possible to identify tendencies in them to promote or demote particular moral values and norms. It holds, for example, that computer programs can be supportive of privacy, freedom of information, or property rights or, instead, to go against the realization of these values. Such tendencies in computer systems are called 'embedded', 'embodied' or 'built-in' moral values or norms. They are built-in in the sense that they can be identified and studied largely or wholly independently of actual uses of the system, although they manifest themselves in a variety of uses of the system. The embedded values approach aims to identify such tendencies and to morally evaluate them. By claiming that computer systems may incorporate and manifest values, the embedded values approach is not claiming that computer systems engage in moral actions, that they are morally praiseworthy or blameworthy, or that they bear moral responsibility (Johnson, 2006). It is claiming, however, that the design and operation of computer systems has moral consequences and therefore should be subjected to ethical analysis.

The use of any technological artefact comes with its own consequences (built-in consequences) what matters is how they arise, that is, central use or peripheral uses. For systems intended to be deployed for public use at a very large scale such as is the case for e-services in e-government it is recommended that systems should be designed in such a way as to minimize the manifestation of negative built-in central use consequences through the embedded values approach.

The advent of Artificial Intelligence (AI), which is classified as an emerging technology in ICT (Stahl and Flick, 2016), has both twisted the ethical issues narrative and legitimized the debate of

the morality of ICT artefacts on their own even without any interaction with users. Bostrom and Yudkowsky (2011), note that the possibility of creating thinking machines raises a host of ethical issues. It is therefore recommended in this study that the topic of ethical issues should start to sit top on the agenda of policy makers and funders to ensure that the systems designed to offer public service such machines do not harm, physically or emotionally, humans and other morally relevant beings, and to the moral status of the machines themselves.

To ensure adherence to the embedded values approach or VSD, it is also further recommended that e-government implementing authorities and all stakeholders involved encourage the promotion of Responsible Research and Innovation (RRI) in ICT research and innovation to possible ethical issues.

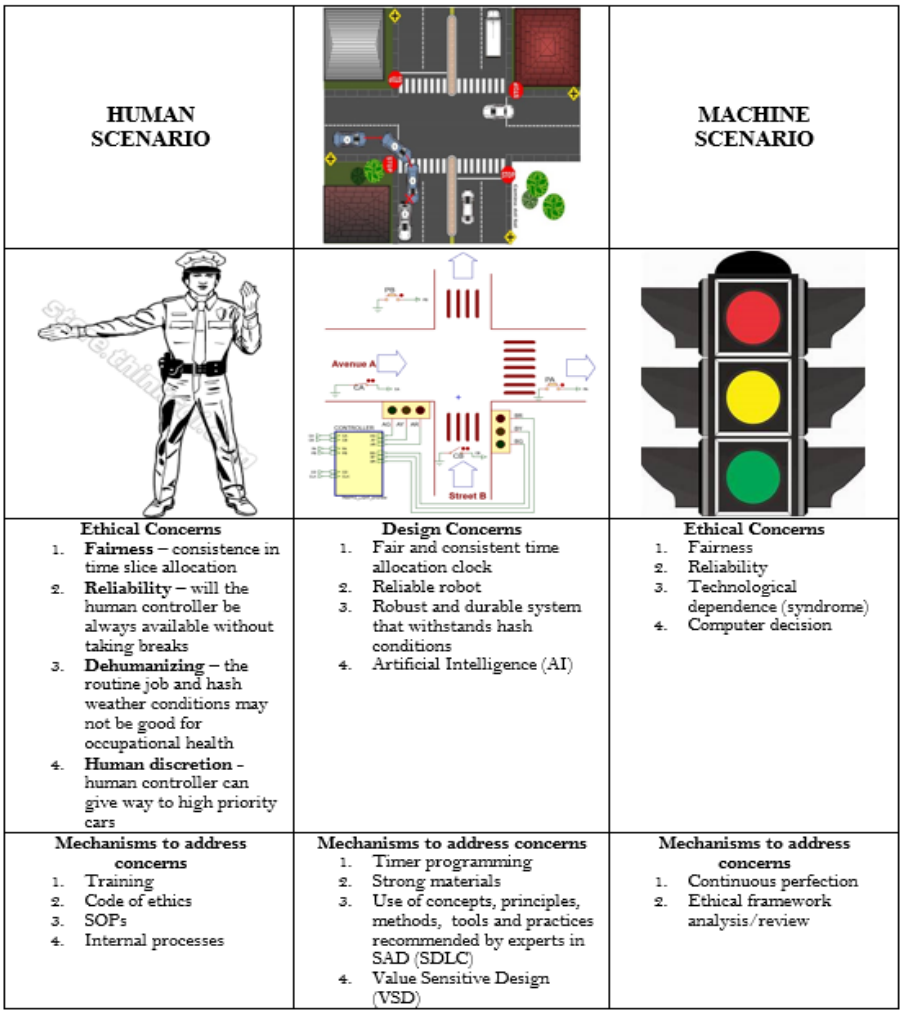

Fig 5.1: The Human-Robot Traffic Control Scenario

For the current study, the researcher develops and recommends the above figure which demonstrates how VSD can be used to embed values in systems meant to provide public service in e-government. In the Human-Robot Traffic Control Scenario for instance, the ethical concerns that arise when a human operator provides a service (in this case a traffic officer) are identified in the Human Scenario and the design equivalent of the ethical concerns identified for each ethical issue. Thereafter, these are embedded in the developed system such that the concerns are all taken care of. For instance, when selecting the materials to use in building the system,

stronger materials that are all-weather proof are chosen and the actual coding a robust programming language is used so that the system, in the Robot Scenario, will manifest a behavior that conforms to expectations of the users in addressing the previously identified ethical concerns which is reliability.

5.2.5 Professional Regulation for G2E

According to the study, professional regulation can help solve some of the ethical issues that arise in e-government implementation not only in developing countries like Zambia, but also anywhere as long as human beings are involved. Where professional regulation is effected, citizens will also have increased trust and confidence in the government electronic services. This means that other than the design of systems that address the ethical issues that arise in the use of ICTs, policies to regulate ethical conduct of the government employees as they design systems and access the systems to provide a service to citizens will also increase e-government implementation success. In this case, the activities of the IT employees as they design the systems as well as the IT and non IT professionals as they use the systems to provide services to citizens all make up the G2E interactions of e-government. While other professionals have their own professional requirements, the professional regulation emphasized in this study is that of the IT employees.

It is therefore recommended from this study that a framework for the regulation of IT professionals should be part of an e-government implementation strategy in order to increase e-government success through citizens' confidence and trust building. The researcher also recommends that the computing profession should be recognized as a formal profession just like the traditional professions such as engineering, law, medicine, accounting among others.

According to Loui and Miller (2008), the obligations of computing professionals are similar to the obligations of other technical professionals, such as civil engineers. Taken together, these professional obligations are called professional ethics. Professional ethics are principles that guide professionals in decision making during their course of duty. These are normally stipulated in a code. Kizza (ibid) notes that the observance of a code of conduct is part of the three basic professional requirements. The other two are;

- A set of highly developed skills and deep knowledge of the domain and
- Autonomy.

A working professional usually observes four types of codes. These are;

i. Professional code,

ii. Personal code,

iii. Institutional code, and

iv. Community code

Computing professionals perform a variety of tasks: they write specifications for new computer systems, they design instruction pipelines for superscalar processors, they diagnose timing anomalies in embedded systems, they test and validate software systems, they restructure the back-end databases of inventory systems, they analyze packet traffic in local area networks, and they recommend security policies for medical information systems. Computing professionals are obligated to perform these tasks conscientiously because their decisions affect the performance and functionality of computer systems, which in turn affect the welfare of the systems' users directly and that of other people less directly. For example, the software that controls the automatic transmission of an automobile should minimize gasoline consumption and, more important, ensure the safety of the driver, any passengers, other drivers, and pedestrians. In short

their responsibilities to society have become so enormous that they cannot be performed by a group of individuals who are free moral agents.

Quinn (2014, p412) postulates that the ability to cause harm to members of the public is a powerful reason why those in computer-related careers must act according to ethical principles. Without formal certification and licensing and other components of a well-developed profession to rely upon, those in computer-related careers must take more personal responsibility for developing their ethical decision-making skills.

The Therac-25 (Leveson, 2017) and the Boeing 737 Max MCAS (Travis, 2019) tragedies serve as examples. In both cases software design error have been cited to have been behind the accidents. In this study, it is recommended that the software designer must be ready to be held responsible and accountable for the inbuilt errors exhibited by the system they have designed just as the user of a system must also be held for the abuse of the privileges in the use of a system as well as human errors attributed to their negligence. Because of their roles in developing software systems, software engineers have significant opportunities to do good or cause harm, to enable others to do good or cause harm, or to influence others to do good or cause harm. To ensure, as much as possible, that their efforts will be used for good, software engineers must commit themselves to making software engineering a beneficial and respected profession. In accordance with that commitment, software engineers should adhere to a Code of Ethics and Professional Practice.

5.3 Areas of Further Research

This research was not exhaustive and hence the areas of further research recommended include the following:

a) A similar research needs to be carried out in the rural districts of the countries to have a more representative picture of the ethical concerns and how these are impeding the adoption of electronic services by the rural communities.
b) There is need to also carry out a study to establish whether current systems deployed for e-government address all the ethical concerns raised in their use, to what extent they address the ethical issues and how the mechanisms put in place have helped raise the adoption levels by citizens nationwide.
c) A detailed study of the philosophical framework of the ethical concerns of citizens in e-government implementation in general.
d) A more detailed study of how the ethical concerns vary across age groups of the society and the development of value sensitive design which maximize the adoption tendencies of different groups according to identified ethical issues.

5.4 Chapter Summary

Ethical issues have a huge impact on e-government implementation success not only in developing countries but developed countries as well as the border on moral decisions make in the use of ICTs. The addressing of the ethical issues that arise in the use of ICTs by governments for public service provision will increase the adoption of these services by citizens. The most prominent ethical issues are security and privacy in that order.

A holistic approach to the addressing of these ethical issues should be adopted by governments to avoid formulation of policies in silos. The design of such policies must precede any systems design as systems design must manifest efforts to address the ethical issues that arise in the use of the particular system concerned. Professional regulation will also increase the trust and

confidence the citizens will have in the systems designed by a regulated cadre of government employees.

6.0 REFERENCES

Palvia, S.C.J. & Sharma, S.S., 2007, E-Government and E-Governance: Definitions/Domain Framework and Status Around the world, Computer Society of India.

Quinn M.J., 2014, Ethics for the information age, 6th Edition, Addison Wesley, p51.

http://www.businessdictionary.com/definition/ethical-issue.html. [19/10/19 21:05]

Meridith Levinson, When Failure is not an Option, CIO Magazine (June 1, 2006) https://www.cio.com/article/2446386/project-management---when-failure-is-not-an-option.html [14/12/19]

Manda, M.I. & Backhouse, J., 2016, Addressing trust, security and privacy concerns in E-government integration, interoperability and Information sharing through policy: a case of South Africa, Association for Information Systems, AIS Electronic Library (AISeL)

Farelo, M. & Morris, C., 2006, The Status of E-government in South Africa https://www.semanticscholar.org/paper/Status-of-E-government-in-South-Africa-Farelo-Morris/884a402e999238310f982f6235bd0d8c07aca687 [09/06/20]

Twizeyimana, J D., Larsson, H., Grönlund, Å., 2018, E-government in Rwanda: Implementation, Challenges and Reflections, Electronic Journal of e-Government, 16(1): 19-31

Gajendra Sharma, 2014, E-Government, E-Participation and Challenging Issues: A Case Study, Kathmandu University School of Engineering Dhulikhel, Kavre, Nepal

Singh H., 2017, what is the difference between e-Government and e-Governance? https://www.jagranjosh.com/general-knowledge/what-is-the-difference-between-egovernment-and-egovernance-1503018565-1 [14/12/19]

Kenneth E. Himma and Herman T. Tavani, 2008, The Handbook of Information and Computer Ethics, John Wiley & Sons [p49]

Allen S Lee, 2010, Retrospect and prospect: information systems research in the last and next 25 years, Journal of Information Technology, p344

Joseph Migga Kizza, 2007, Ethical and Social Issues in the Information Age, 3rd Edition, Springer Science and Business Media, p38

Republic of Zambia, Cabinet Office, Smart Zambia E-Government Master Plan (2016 -2020)

Hilary Mullen, David Sanford Horner, 2004, Ethical Problems for e-Government: An Evaluative Framework, Electronic Journal of e-Government Volume 2 Issue *3* 2004, p1

ZICTA, 2018, National Survey on Access and Usage of Information and Communication Technologies by Households and Individuals - Preliminary Report, p55.
The Republic of Zambia, Ministry of Communications and Transport, National Information and Communications Technology Policy 2006, p6

Bernd Carsten Stahl, 2005, The Ethical Problem of Framing e-Government in Terms of e-Commerce, Centre for Computing and Social Responsibility, De Montfort University, UK

Anil Kumar Pandey, 2015, Prospects of Social Networking Services in Implementation of E-Governance, Computer Centre, Banaras Hindu University, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2015): 78.96, Impact Factor (2015): 6.391

Naim Kapucu (2007), Ethics of Digital Government, University of Central Florida, USA

Arief Ramadhan, Dana Indra Sensuse, Aniati Murni Arymurthy, 2011, e-Government Ethics : a Synergy of Computer Ethics, Information Ethics, and Cyber Ethics, Faculty of Computer Science, University of Indonesia, Depok, Indonesia, *(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 8, 2011*

Göran Goldkuhl, 2012, From policy to design and effects: A framework for e-government research, Department of Management and Engineering, Linköping University, Sweden & Department of Computer & Systems Sciences, Stockholm University, Sweden.

Luciano Floridi, 2010, The Cambridge Handbook of Information and Computer Ethics, Cambridge University Press

E-Government toolkit for developing countries: UNESCO 2005, p9

ITU e-Government Implementation Toolkit; A framework for e-government readiness and action priorities 1, 2009, p4, http://www.itu.int/ITU-D/cyb/app/e-gov.html

"Moral Relativism." Internet Encyclopedia of Philosophy. http://www.utm.edu/research/iep/ni/m-ration.html https://www.iep.utm.edu/ethics/ [15/12/19]

Oxford Advanced Learner's Dictionary, International Student Edition, 9th Edition, 2015

Ugbogbo S.N. and Atu O.M., 2016, Ethical Issues In Information Technology, 'A Conceptual Approach", Igbinedion University Journal of Accounting, Vol. 2 August, 2016

Shalini Verma Sheel and Neelaksh Sheel (2017), E-governance: Challenges in the way ahead, Meerut Institute of Engineering and Technology (India), JP Institute of Engineering and Technology (India), International Journal of Science, Technology and Management, Vol. no. 6, Issue no. 2 www.ijstm.com [15/12/19]

Kalam Abdul A.P.J., 2006, Address at the inauguration of the Biennial Conference of Anti-Corruption/Vigilance Bureaus of States, UTs and Officers of the CBI, 16 Nov 2006. Source: http://www.cbi.gov.in/ https://shodhganga.inflibnet.ac.in/bitstream/10603/19278/6/06_chapter%201.pdf [15/12/19]

Kolachalam S., 2002, An Overview of E-Government, Conference: International Symposium on Learning Management and Technology Development in the Information Age, At University of Bologna (Bologna-Italy), Volume: Accademia di Economia Aziendale Italiana, Business and Managment Sciences International Quarterly Review. No. 1, 2004, pp 1-12. International Association Europe and Asia, 2003.

Sunitha, 2007, E-government in developing countries (Opportunities and Implementation barriers) Lulea University of Technology

The E-government Handbook for developing countries, 2002, Information for Development Program, Center for Democracy and Technology

Ndou, V. (2004). E-government for developing countries: Opportunities and challenges, The Electronic Journal of Information Systems in Developing Countries, 18.

Heeks, R. (2001). Understanding e-governance for development: Institute for Development Policy and Management Manchester.

Shailendra Singh & Singh Karaulia, 2011, E-Governance: Information Security Issues, International Conference on Computer Science and Information Technology (ICCSIT'2011) Pattaya.

Lupiya Simusokwe, 2009, Cybercrime and the Law in Zambia, University of Zambia

ICT Act 2009, Laws of Zambia

ECT Act 2009, Laws of Zambia

ICTAZ Act 2018, Laws of Zambia

Simusikwe L., 2009

Copyright Act 1994, Laws of Zambia

https://www.merriam-webster.com/dictionary/artificial%20intelligence [02/06/20]

Bostrom N, & Yudkowsky E., 2014, Forthcoming. "The Ethics of Artificial Intelligence." In Cambridge Handbook of Artificial Intelligence, Edited by Keith Frankish and William Ramsey New York: Cambridge University Press

Maner, W. (1980[1978]). Starter Kit on Teaching Computer Ethics. Self-published in 1978, published in 1980 by Helvetia Press in cooperation with the National Information and Resource Center on Teaching Philosophy, Hyde Park, NY.

Qiao Liang and Wang Xiangsui, 2002, Unrestricted Warfare: China's Master Plan to Destroy America (Panama: Pan American Publishing Company

Allan B. Carroll, 2014, The critical vulnerability of Technological dependence: a culturally Driven phenomenon, United States Army, School of Advanced Military Studies, United States Army Command and General Staff College, Fort Leavenworth, Kansas.

Parnas, David, John van Schouwen, and Shu Kwan. “Evolution of Safety-Critical Software.” *Communications of the ACM,* 33(6), 1990, pp. 636–648.

Jean Damascene Twizeyimana and Annika Andersson, 2019, The public value of E-Government – A literature review, Government Information Quarterly
http://www.elsevier.com/locate/govinf

Rose, J., Persson, J. S., & Heeager, L. T., 2015, How e-Government managers prioritise rival value positions: The efficiency imperative. *Information Polity, 20*(1), 35–59.https://doi.org/10.3233/IP-150349.

Rose, J., Persson, J. S., Heeager, L. T., & Irani, Z., 2015, Managing e-Government: Value, positions and relationships. *Information Systems Journal, 25*(5), 531–571. https://doi.org/10.1111/isj.12052.

Chircu, A. (2008). E-government evaluation: Towards a multidimensional framework. Electronic Government, *5*(4), 345–363. https://doi.org/10.1504/EG.2008.019521.

Bannister, F., & Connolly, R. (2014). ICT, public values and transformative government: A framework and programme for research. *Government Information Quarterly*, *31*(1), 119–128. https://doi.org/10.1016/j.giq.2013.06.002.

Mkude, C. G., & Wimmer, M. A. (2013). Strategic framework for designing e-government in developing countries. In M. A. Wimmer, M. Janssen, & H. J. Scholl (Vol. Eds.), Electronic government: Proceedings of the 12th IFIP WG 8.5 international conference, EGOV 2013. Vol. 8074. Electronic government: Proceedings of the 12th IFIP WG 8.5 international conference, EGOV 2013 (pp. 148–162). (Koblenz, Germany)

Grimsley, M., & Meehan, A. (2007). E-government information systems: Evaluation-led design for public value and client trust. European Journal of Information Systems, 16(2), 134–148. https://doi.org/10.1057/palgrave.ejis.3000674

Moor, J. H. 1998. ‘Reason, Relativity and Responsibility in Computer Ethics’, Computers and Society 28(1), 14–21.

https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security [15/12/19]

John Locke, 1988, Two Treatises of Government, Cambridge University Press, Cambridge, England.

Rawls, J. (1999). A Theory of Justice, revised edition. Oxford University Press, Oxford.

Luciano Floridi (2010), "*Foundations of Information Ethics*" in Himma K.E. & Tavani H.T, 2008, The Handbook of Information and Computer Ethics, John Wiley & Sons, p3

Belinda Davis Lazarus, 2007, (University of Michigan – Dearborn, USA), Encyclopaedia of Information Ethics and Security, Ethics and Access technology for persons with disability

The E-Government for Developing Countries, 2002, A Projevt of InfoDev and Center fod Democracy and Technology, CDT, www.cdt.org

Fraunholz, B., & Unnithan, C. (2008, November 16). Anti-apathy approaches in representative democracies: e-governance and web 2.0 – facilitating citizen involvement? *International Journal of Electronic Democracy*, *1*(1), 51–84. doi:10.1504/IJED.2008.021278

Abid Thyab Al Ajeeli and Yousif A. Latif Al-Bastaki, 2011, Handbook of Research on E-Services in the Public Sector: E-Government Strategies and Advancements, p28, p88

Sharma Gajendra, Bao Xi and Qiang Wang, 2012, E-Government: Public Participation and Ethical Issues, Journal of E-Governance 35 (2012) 195–204, Dalian University School of Technology, China

K. Chopra and W.A. Wallace, 2003, Trust in Electronic Environments, In: Thirty sixth Hawaii International Conference on System Sciences (HICSS), Maui, Hawaii.

Gajendra Sharma, 2014, E-Government, E-Participation and Challenging Issues: A Case Study, Kathmandu University School of Engineering Dhulikhel, Kavre, Nepal

Bernd Carsten Stahl, 2005, The Ethical Problem of Framing e-Government in Terms of e-Commerce, Centre for Computing and Social Responsibility, De Montfort University, UK

Ess, C. 'The Political Computer: Democracy, CMC, and Habermas', 1998, In: Philosophical Perspectives on Computer-Mediated Communication, Ess, Charles (ed.), pp. 187 - 230, State University of New York Press, Albany, 1996

John Stuart Mill. "On Liberty." In *On Liberty and Utilitarianism*. Bantam Books, New York, NY, 1993.

Samson, Jeri and Keen, Beth (2006). "Internet addiction". Available at: http://www.notmykid.org/parentArticles/internet/

Reynolds G. W, 2014, Ethics in Information Technology, 5th Edition, Cengage Learning, US

Hilary Mullen, David Sanford Horner, 2004, Ethical Problems for e-Government: An Evaluative Framework, Electronic Journal of e-Government Volume 2 Issue *3* 2004, p1.

Arief Ramadhan, Dana Indra Sensuse, Aniati Murni Arymurthy, 2011, e-Government Ethics : a Synergy of Computer Ethics, Information Ethics, and Cyber Ethics, Faculty of Computer Science, University of Indonesia, Depok, Indonesia, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 8, 2011.

https://www.szi.gov.zm [18/11/19, 20:54].

Deloitte Consulting LLC, 2000, At the Dawn of e-Government: The Citizen as Customer, Deloitte Research, 1633 Broadway, New York, New York 10019

Misra D. C. I.A.S. (Retd.), 2006, 10th National Conference on e-Governance, February 2-3, 2006, Bhopal, Madhya Pradesh, India (http://www.10thnationalegovconf.in/14.pdf)

Himma K.E. & Tavani H.T, 2008, The Handbook of Information and Computer Ethics, John Wiley & Sons, p69.

Friedman, B., Millett,L., and Felten, E., 2000, Informed Consent Online: A Conceptual Model and Design Principles. University of Washington Computer Science & Engineering Technical Report 00–12–2.

Millett, L., Friedman, B., and Felten, E. (2001). Cookies and web browser design: Toward realizing informed consent online. In: Proceedings of CHI 2001. ACM Press, pp. 46–52.

Frankenfield J., 2019, Artificial Intelligence (AI)
https://www.investopedia.com/terms/a/artificial-intelligence-ai.asp [14/12/19]

Michael C. Loui and Keith W. Miller, 2008, Ethics and Professional Responsibility in Computing, University of Illinois

Twizeyimana, J.D., 2017, September. User-centeredness and usability in e-government: a reflection on a case study in Rwanda. In Proceedings of the Internationsl Conference on Electronic Governance and Open Society: Challenges in Eurasia (pp. 172-178). St. Petersburg, Russia, September 04 - 06, 2017. New York:ACM. , p.172, pp.174- 175

Laudon K, Laudon J, 2008, Management Information Systems, *Managing the digital firm*, 10th Edition, Prentice Hall of India, p514

https://www.surveysystem.com/sscalc.htm

Resnik et al., 2011, Environmental Health Ethics, Cambridge University Press, UK, Introduction to Educational Research, http://www.southalabama.edu/coe/bset/johnson/lectures/lec2/p9

https://docs.google.com/forms/d/1xWEKnQ0cTpcQnt4LiiYVxp3EXqneU2Ef8bmQn5b2_8/edit#responses.

Mjumo Mzyece, 2012, A Critical Analysis of e-Government in Zambia, French South African Institute of Technology (F'SATI), Tshwane University of Technology, South Africa

Wiener, N. (1985). The machine as threat and promise. In: Masani, P. (Ed.), Norbert Wiener: Collected Works and Commentaries, Vol. IV. The MIT Press, Cambridge, MA, pp. 673–678. Reprinted from St. Louis Post Dispatch, December 13, 1953.

Nissenbaum, H. (1998). Values in the design of computer systems. Computers and Society, 1998, 38–39.

Flanagan, M., Howe, D., and H. Nissenbaum, H. (2007). Values in design: theory and practice. In: van den Hoven, W.J. and Weckert, J. (Eds.), Information Technology and Moral Philosophy. Cambridge University Press, Cambridge UK.

Johnson, D.G. (2006). Computer systems: moral entities but not moral agents. Ethics and Information Technology, 8(4), 195–204.

Bernd Carsten Stahl*, Job Timmermans and Catherine Flick (2016), Ethics of Emerging Information and Communication Technologies: On the implementation of responsible research and innovation, Centre for Computing and Social Responsibility, De Montfort University, The Gateway, Leicester, LE19BH, UK

Nancy G. Leveson, 2017, The Therac-25: 30 Years Later, MIT https://www.computer.org/csdl/magazine/co/2017/11/mco2017110008/13rRUxAStVR [05/12/19]

Gregory Travis, 2019, How the Boeing 737 Max Disaster Looks to a Software Developer https://spectrum.ieee.org/aerospace/aviation/how-the-boeing-737-max-disaster-looks-to-a-software-developer [05/12/19]

APPENDICES

Appendix I: Questionnaire

The online questionnaire can be found on the URL below;

https://docs.google.com/forms/d/1xWEKnQ0cTpcQnt4LiiYVxp3EXqneU2Ef8bmQn5b2_8/edit#responses

THE UNIVERSITY OF ZAMBIA

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING

STUDENT NAME: Eddie Liywalii

COMPUTER NUMBER: 2017014698

Questionnaire

Dear respondent,

I am a student at the University of Zambia in the School of Engineering. I am carrying out a research on Analysing the Impact of Ethical Issues on E-Government Implementation: A Case Study of Zambia. You have been randomly selected and it is my sincere request that you answer the following questions honestly. Kindly note that the information collected from you will be treated with utmost confidentiality and will only be used for the purpose of this research. Your participation will highly be appreciated.

INSTRUCTIONS

- DO NOT write your name on the questionnaire
- Where options are provided, simply tick within the given space. For instance

  Do you live in Lusaka? Yes [√] No [ ]

	SECTION A **PERSONAL DETAILS**	**For Official Use Only**
1	Sex Male [ ] Female [ ]	[ ]
2	Marital Status Married [ ] Separated [ ] Widows [ ] Single [ ] Divorced [ ]	[ ]
3	Age ……	
4	Do you have a family (Wife/husband, children, dependents)? Yes [ ] No [ ]	[ ]
5	If your answer to question 3 is yes, kindly state the family size 2 people [ ] 3 people [ ] 4 people [ ] Above 4 people [ ]	[ ]
6	What is your ethnicity? Bantu [ ] Arabic [ ] Caucasian [ ] Asian [ ] Latino [ ] Other [ ], Specify other ……	[ ]
7	What is your religion? Christian [ ] Hindu [ ] Muslim [ ] Jewish [ ] Other [ ], Specify other ……	[ ]

	ACADEMIC DETAILS	
8	What is the highest level of education that you have attained? No formal education [ ] Primary [ ] Secondary [ ] College Diploma/Certificate [ ] University Degree [ ]	[ ]
9	What is the area of study for your post-secondary education? Public Administration [ ] Economics [ ] Library/IS [ ] Law [ ] Education Arts [ ] Education Sciences [ ] Engineering [ ] Computer Science/IT [ ] Business/Accounts [ ] Others [ ], specify …….	[ ]
10	What is your level of responsibility in the organization you work for? Director [ ] Manager [ ] Supervisor [ ] Worker [ ] Other [ ], specify other ……..	[ ]
11	How would you classify your role? Policy making [ ] Policy analysis [ ] Policy Implementation [ ] Regulation [ ] Other [ ], specify other ……	[ ]

	SECTION B **E-GOVERNMENT RELATED QUESTIONS**	
12	Does Zambia as a country have an E-government policy? Yes [ ] No [ ]	[ ]
13	If your answer to 12 is yes, does the Zambian E-government Policy address any ethical issues that may arise in the implementation of e-government? Yes [ ] No [ ]	[ ]
14	Mention any five (5) of the ethical issues in the e-government policy i. …….. ii. …….... iii. …….. iv. …….. v. ……..	[ ]
15	If the e-government policy does not include ethical issues arising in e-government implementation, are there plans to address these issues? Yes [ ] No [ ]	[ ]
16	Which of the following is the major challenge in implementing e-government? a) Funding b) Political will c) Citizen ICT literacy levels d) Policy e) Infrastructure f) Ethical issues g) Other (State) ……..	[ ]

17	How relevant to e-government implementation do you think ethical issues are? a) Irrelevant b) Fairly relevant c) Relevant d) Very relevant	[ ]
18	Do you feel that the current ICT policies (other than e-government policies/bills/acts) adequately address ethical issues that arise in e-government implementation? a) Disagree b) Fair agree c) Agree d) Strongly agree	[ ]
19	What ethical areas or issues do you feel are addressed by the policies/bills/acts based on your answer to question 18? …….... …… ……	[ ]
20	By your own assessment, what do you feel are the ten (10) major ethical issues in e-government implementation? …….. …….. …….. …….. …….. …….. …….. …….. …….. ……..	[ ]

	IMPACT OF ETHICAL ISSUES ON E-GOVERNMENT	
21	Would e-government result in improved efficiency in government administration and service delivery to citizens? a) Disagree b) Fairly agree c) Agree d) Strongly agree	[ ]
22	Would the inclusion of ethical issues contribute to the successful implementation of e-government? a) Disagree b) Fairly agree c) Agree d) Strongly agree	[ ]
23	Do you think that the addressing of ethical issues in e-government implementation increases citizens/businesses embracing of e-government? a) Disagree b) Fairly agree c) Agree d) Strongly agree	[ ]
24	Do you feel that policy makers and analysts possess adequate knowledge of ethical issues that arise in e-government implementation in developing countries such as Zambia? a) Disagree b) Fairly agree c) Agree d) Strongly agree	[ ]

25	What IT training do you think provides this adequate knowledge in IT ethics particularly relating to e-government? …….. …….. …….. **<u>SYSTEMS ADDRESSING ETHICAL ISSUES</u>**	[ ]
26	Do you think information systems in e-government could be designed in such a way as to address ethical issues that arise in e-government? a) Disagree b) Fairly agree c) Agree d) Strongly agree	[ ]
27	Do feel that the designing of information systems that address ethical issues is preceded by a policy framework that addresses ethical issues? a) Disagree b) Fairly agree c) Agree d) Strongly agree	[ ]
28	How do you feel systems in e-government could be designed to address each of the ethical issues identified in question 20? *(Ethical issue)* *(System design)* …….. …… …….. …… …….. …… …….. …… …….. …… …….. ……... …….. …… …….. ……... …….. …… …… ……	[ ]

29	Do developers as IT professionals who design and build these systems have a role in addressing ethical issues that arise in e-government? Yes [ ] No [ ]	[ ]
30	If your answer to 29 is yes, what role do you think IT professionals play in addressing these ethical issues? (*Tick as appropriate*) a) Commitment [ ] b) Integrity [ ] c) Responsibility [ ] d) Accountability [ ] e) All of the above [ ]	[ ]
31	Do you feel professional regulation will help achieve the realization of the above values in the IT professionals? a) Disagree b) Fairly agree c) Agree d) Strongly agree	[ ]
32	Will this in any way impact public perception for IT professionals? Yes [ ] No [ ]	[ ]
33	Will this increase the confidence and trust in information systems designed for e-government? a) Disagree b) Fairly agree c) Agree d) Strongly agree	[ ]

34	For e-government to succeed in general, do you think it is vital for IT professionals to firmly understand ethical issues that arise in e-government? a) Disagree b) Fairly agree c) Agree d) Strongly agree	[ ]
35	Currently, do ICT policies and the regulatory framework adequately address professional and ethical issues for e-government implementation? a) Disagree b) Fairly agree c) Agree d) Strongly agree	[ ]
36	What do you feel should be done to address ethical issues that arise in e-government implementation? …… …… …… …… …… …… ~~~~~~~~~~~~~~~~~~~~~~~~THANK YOU~~~~~~~~~~~~~~~~~~~~	