Information privacy and data protection in e-government services in The Gambia: A human rights perspective

Nasiru Deen

Submitted in partial fulfilment of the requirements for the degree of MA
Erasmus Mundus Human Rights Practice and Policy Masters Programme

School of Global Studies, University of Gothenburg
Pedro Arrupe Human Rights Institute, Deusto University
School of Humanities and Social Sciences, University of Roehampton
Department of Social Sciences, University of Tromsø – Arctic University of Norway

[May 2024]

Dissertation Module (30 ECT)

Supervisor: **Damon Barrett**

Spring semester 2024

Table of Contents

Acknowledgements 2
Abstract 3
Chapter 1: Introduction to E-government in The Gambia 4
1.1 Background 4
1.2 Research Question 5
1.3 Rationale for the Research 5
1.4 Relevance to Human Rights 6
1.5 Research Methodology 7
1.4.1 Study Design 7
1.4.2 Selection of participants 8
1.4.3 Data collection and analysis 9
1.4.4 Ethics 10
1.6 Literature Review 11
1.6.1. E-government Implementation 11
1.6.2. Information Privacy and Data Protection: Legal and Technical Perspective 13
1.7 Theoretical Framework 14
Chapter 2: Information privacy and data protection- a human rights issue. 16
2.1 Introduction 16
2.2 Global Instruments for Information Privacy and Data Protection 16
2.3 The EU and Instruments for Information Privacy and Data Protection 19
2.4 African Instruments for Information Privacy and Data Protection 22
2.5 Legal instruments in The Gambia for Information Privacy and Data Protection 25
Chapter 3: Findings on e-government services in The Gambia. 29
3.1 Introduction 29
3.2 Inadequate framework and inadequate infrastructure for privacy and data protection in The Gambia 29
3.3 Lack of transparency and accountability in e-government service implementation 31
3.4 Non-adherence to the principle of data minimisation in The Gambia 32
3.5 Improved data-sharing within government as a goal of e-government 33
Chapter 4: Discussion of findings 35
Conclusion & opportunities for further research. 41
Bibliography 43
Annexes 50

Acknowledgements

Thanks goes to my supervisor Damon Barrett for his exceptional supervision of this thesis. I could not have been assigned better supervision. I also wish to express my gratitude to the key informants who provided the crucial data for this research. Additionally, I am thankful to the EMHRPP consortium for offering me the opportunity to participate in this program and to learn from esteemed human rights scholars. I am also deeply appreciative of the moral support from my family and the remarkable cohort of the EMHRPP program (2022-2024).

Abstract

This study undertakes an investigation into the standards of information privacy and data protection within the framework of e-government implementation in The Gambia. The Government of The Gambia has embarked upon the deployment and operation of e-government services across various state agencies, aiming to facilitate crucial transactional processes, notably the issuance of ID cards and passports. However, the execution of these services inherently entails the aggregation of substantial volumes of personal data, posing the risk of violation of the right to information privacy. To mitigate this threat, the adoption of robust information privacy and data protection mechanisms is imperative. Using a doctrinal approach and through semi-structured interviews with five key informants, this thesis scrutinizes the presence and efficacy of such mechanisms within the context of The Gambia's e-government milieu, benchmarking against established global human rights standards. The findings reveal significant gaps concerning information privacy and data protection within e-government services in The Gambia, leading to their failure to meet recognized standards of human rights. The thesis further enriches the theoretical framework on engineering for human rights by demonstrating the paramount importance of governmental oversight in comparison to the role of engineers. It concludes that governments wield a greater influence in ensuring the design and operation of e-government services align with recognized human rights standards, particularly regarding information privacy and data protection.

Word Count: 15, 980

Chapter 1: Introduction to E-government in The Gambia

1.1 Background

In 2022, The Gambia became the first African country with a fully digital immunization register. The new health information management system assists the Ministry of Health (MoH) of The Gambia in digitally tracking all children under five regarding vaccines. This system implemented a new hybrid paper-digital solution that collects, shares, stores, and distributes data for the Gambia's Expanded Programme for Immunization (EPI) using Smart Paper Technology (SPT). The data is digitized through the SPT engine and stored in an electronic register from which health management information system (HMIS) reports are generated and shared at health facility, regional, and national levels (Global-Voices, 2022). Some benefits of the system include the automatic generation of request forms for the delivery of vaccines to health centres, sending of SMS messages to remind parents of vaccination appointments for their infants, and making follow-ups for infants who fail to meet the prescribed vaccination schedule (Global-Voices, 2022).

Previously, the government of the Gambia had rolled out the country's first ever digital birth and health insurance certificates, aiming to enhance health outcomes, improve healthcare access, and ensure citizens' access to digital documents at any time. The initiative involved a three-month citizen registration process across the country, provided at no cost to citizens. The collected data, which includes names, residence, date, and place of birth, as well as parental identity, is said to be confidential and stored in an online system managed by the State (HealthCare Africa, 2022). This data has the potential to provide the government with relevant statistics on the Gambian population, facilitating the development and implementation of national policies, including demographic distribution by age, sex, and residence.

In addition, the previous government of Yahya Jammeh, had in 2016 contracted the Belgian based Semlex group to develop and operate a biometrics system that would be used to produce and issue national ID cards, driving licenses, visa stickers, and residential permits. Semlex has and continues to provide similar services in other countries predominantly in developing parts of the world (Government of The Gambia, 2016). The system implemented by Semlex in the Gambia collects biometric data from persons who require these services i.e. the production of IDs, driving licenses etc. This data includes fingerprints, and facial images in addition to other personal data such as names and addresses (Biometric-Update, 2018).

The Gambian government also contracted Comfort Quality Services Ltd to produce aluminium number plates and QR code car stickers and to deliver QR scanners to the Gambia Police Force. These scanners will be used by road traffic officers to scan the QR codes on the new stickers that every car in The Gambia would be required to have. This scanning process will provide access to accurate vehicle and motorcycle details, aiding in routine security checks and vehicle verification. The technology will also assist the police in addressing vehicle-related crimes and incidents more effectively (The Standard Newspaper, 2020).

These e-government services are currently being implemented by the government of The Gambia in collaboration with private sector developers. However, the proliferation of these e-government systems, which involve the collection, processing, and storage of personal data, raises significant concerns regarding privacy and data protection. The dearth of academic research and literature on whether these installed e-government systems in The Gambia incorporate adequate mechanisms for privacy and data protection, in accordance with international human rights standards and global best practices, further underscores the importance of this inquiry. This study aims to investigate the presence and efficacy of information privacy and data protection measures in the execution of the e-government services in The Gambia, to determine whether their data processing operations adhere to internationally recognized human rights standards and best practices for information privacy and data protection.

1.2 Research Question

What measures for information privacy and data protection exist in the operations of e-government services in The Gambia? Do they meet recognised standards of human rights and best practice?

1.3 Rationale for the Research

The rationale for my research is underpinned by the diffusion of innovations model (Rogers, 2005). This model consists of five crucial stages essential for the adoption of an innovation. It commences with the knowledge stage, where individuals strive to comprehend the nature and functionality of the innovation. Key inquiries such as "What is the innovation?" "How does it work?" and "Why does it work?" are paramount concerns once individuals become aware of the existence of an innovation (Rogers, 2005, p. 167). Subsequently, the Persuasion stage ensues as individuals formulate attitudes, whether favorable or unfavorable, towards the

innovation. Following this, the Decision stage transpires as individuals engage in activities leading to the choice to either adopt or reject the innovation. The subsequent stage is the Implementation stage, which entails putting the innovation into practice and adapting it where necessary. Finally, the Confirmation stage occurs, involving the reinforcement of the decision made, potentially reversing it if conflicting messages about the innovation arise (Rogers, 2005, p. 164). As individuals progress through the persuasion and confirmation stages, they persistently seek knowledge to evaluate the innovation and alleviate uncertainties regarding its anticipated outcomes (Ibid).

The Gambia is currently at the implementation stage of the aforementioned model, as several e-government services are currently operational providing transactional services while collecting personal data on a large scale. However, there is a dearth of knowledge on the processes involved in these e-government operations, especially with regards considerations for privacy and data protection rights, with no existing literature providing relevant detailed information on this phenomenon. This lack of knowledge has created uncertainties as to whether these e-government services should continue to operate in the manner in which they do today in The Gambia. As such, the new knowledge that this thesis creates clears these uncertainties to ascertain the existence of these privacy and data protection mechanisms, confirming if they align with international human rights standards. The existence of this knowledge in academic literature could potentially lead to persuasion for reinvention, which Rogers (2003, p. 180) describes as the degree to which an innovation is changed or modified by a user(s) in the process of its adoption and implementation to achieve certain improvements, which in the case of the Gambia's e-government services, could be improvements to incorporate privacy and data protection mechanisms that meet recognised human rights standards. Reinvention usually happens at the implementation stage (Ibid), and as such The Gambia in its current stage of e-government implementation is well situated for a reinvention based on the knowledge this research provides.

1.4 Relevance to Human Rights

This thesis is relevant to human rights, particularly in the context of privacy and data protection. It addresses the critical issue of whether the existing privacy and data protection measures within the operation of e-government services in The Gambia align with recognized standards of human rights and best practice. Human rights, as enshrined in international treaties and conventions, include the right to privacy and the right to the protection of personal data. These

rights are essential for safeguarding individual autonomy, dignity, and freedom from unwarranted intrusion. In the digital age, where governments increasingly collect, process, and store vast amounts of personal data through e-government services, ensuring the protection of the right to information privacy is paramount. This thesis directly interrogates the extent to which the information privacy and data protection measures employed in e-government services in The Gambia adhere to internationally recognized human rights standards. By evaluating the alignment of these measures with human rights principles, this thesis contributes to the broader discourse on the protection of individual rights in the digital sphere. Furthermore, the findings of this research have practical implications for policy and practice in The Gambia and potentially other countries with similar e-government initiatives. By identifying gaps or areas of non-compliance with human rights standards, this thesis informs the development and implementation of policies and measures aimed at enhancing the protection of privacy and data rights in e-government services. Overall, it underscores the fundamental importance of privacy and data protection in the context of human rights, and it seeks to address pressing issues related to the implementation of e-government services while ensuring the preservation of these rights.

1.5 Research Methodology

1.4.1 Study Design

This thesis utilizes the case study research methodology. According to Yin (2009), a case study is an empirical investigation that delves into a contemporary phenomenon in-depth and within its real-life context, particularly when the boundaries between the phenomenon and its context are not clearly evident. Case study methods is highly relevant to this research, as the implementation of e-government systems occurs within a multifaceted context characterized by intricate socio-political, economic, legal, and technological factors that are currently unidentified in academic literature, especially with regards to how they affect the extent to which privacy and data protection practices are embedded within the e-government services in The Gambia. Yin further explains that case study methodology is also relevant if the research questions "require an extensive and in-depth description of some social phenomenon" (ibid, p.4), which is what this thesis seeks to do. Contextually speaking, a number of scholars agree that case studies should be limited to a particular context in order to provide in-depth knowledge (Takahashi & Araujo 2020, p.102). The specific context here is the implementation of e-government services in The Gambia, as there is a current lack of empirical evidence on the extent to which these services incorporate privacy and data protection mechanisms in their

operations. This specific context also allows for the sourcing of experts who can provide relevant data regarding this particular context. Additionally, Otley and Berry (1994, p. 47) emphasize that case study methodology enables researchers to generate new knowledge in situations where existing knowledge is insufficient and incomplete. This assertion further substantiates the use of case study as an appropriate method to address the research question, especially considering the limited or non-existent studies on the extent to which privacy and data protection practices are embedded in e-government services in The Gambia. This method involves using multiple sources of evidence (Yin, 2009 p. 4), and this thesis does utilise several sources of data to answer its research question.

Firstly, this thesis uses the doctrinal approach to examine policy documents, legal instruments, court judgments, and even open-source documents that detail the global human rights standards of privacy and data protection, as well as the current standards within the existing legal and regulatory framework of privacy and data protection in The Gambia. This would establish the human rights standards of privacy and data protection that are expected of any rights respecting data protection regime and provide a benchmark for assessing the extent to which the existing privacy and data protection mechanisms in e-government services in The Gambia (if any) meet these globally recognised standards of best practice. Secondly, in order to ascertain what mechanisms of privacy and data protection currently exist within the operations of these e-government services, insights from relevant stakeholders in the privacy and data protection space in The Gambia, were collected through semi-structured interviews. Through these interviews, this research sought to get insights from persons within government departments, civil society, media and private entities, in order to present a balanced perspective by involving those responsible for implementing e-government services and the rules that govern it (the government in collaboration with some private entities), and those who use or possess knowledge of the use of these services and its impacts, or potential impacts (such as data experts, the media, civil society, etc.). The aim is to present a balanced view of the conditions under which these e-government systems operate in the collecting, processing, and storing personal data, in order to evaluate whether these meets globally recognised human rights standards.

1.4.2 Selection of participants

Guided by set criteria, purposive sampling methods is used to select the interview participants. Purposive sampling is a method ‘used to select respondents that are most likely to yield appropriate and useful information’ (Kelly, 2010 p. 317). Thus, the selection criteria for

participants were grounded in their knowledge of and/or involvement in e-government implementation in The Gambia. These interviews can thus be characterised as key informant interviews, which is used in qualitative research method to provide good information and a deeper insight into a phenomenon occurring around them (Marshall, 1996 p. 92). The key informant technique offers significant advantages due to its ability to gather high-quality data quickly, which contrasts with the time-consuming and costly nature of obtaining equivalent information through in-depth interviews with other community members (Marshall, 1996 p. 93). Ten potential key informants were approached to participate through various means including via LinkedIn messaging, email, and WhatsApp messaging. Out of those, five were eventually interviewed. All of those who refused to be interviewed or did not respond to my request for interview were potential key informants who work for the government of The Gambia in the implementation of e-government services. The five participants included key informants from civil society, media, international development agencies funding the implementation of e-government, and private sector companies designing and implementing these services in The Gambia. For privacy and confidentiality reasons, the interviewees will be named and referenced 'Expert 1 to Expert 5'.

Participant Label	Sector	Description
Expert 1	Multistakeholder technical community	*Expert 1*is represents a prominent multi-stakeholder network on digital governance in the country.
Expert 2	Private	*Expert 2* represents a private company designing and developing e-government services for The Gambia
Expert 3	Investigative Media	*Expert 3* is an investigative journalist.
Expert 4	Law & Regulation	*Expert 4* is a Lawyer specialising in technology law in The Gambia.
Expert 5	Civil Society	*Expert 5* is an activist and civil society actor

Table 1.1 Summary of the participants with their labels

1.4.3 Data collection and analysis

The interview guide found in annex 1 includes questions aimed at getting information that would help answer the research question in this thesis. The questions and rationale behind the questions are included in the guide. Each individual one-to-one interview lasted approximately 30 minutes, and was carried out online using Microsoft teams, and recorded using the Dictaphone app. All interviews were conducted in English, leaving no need for translation. The data analysis process began with the verbatim transcription of interview data. Precautions were

taken to ensure the preservation of participants' anonymity including conducting data anonymisation. Both audio and transcribed data were organized into individual interview folders and labelled as E1 (Expert 1), E2 (Expert 2), and E3 (Expert 3) etc. The transcribed data was reviewed simultaneously with the playback of the recorded interviews. This process allowed for necessary corrections to be made to any mis-transcribed data.

Thematic analysis, which is an approach used to analyse qualitative data by systematically exploring a dataset to recognize, examine, and communicate recurring patterns (Braun and Clarke, 2006), was employed in the analysis of the interviews. It serves as a suitable method for comprehending a collection of experiences, thoughts, or behaviours within a dataset (Braun and Clarke, 2012), which are the categorised into different themes. This thesis employs inductive thematic analysis, which involves exploring data from a data-driven perspective, starting directly from the dataset itself (Braun and Clarke, 2012). This approach allows themes to be generated by the researcher without imposing pre-existing theories or frameworks (Ibid). A theme is a 'patterned response or meaning' (Braun and Clarke 2006, p. 82) providing insights into the research question. A theme is conceived from codes which are the smallest units of analysis that capture interesting features of the data that is potentially relevant to the research question (Braun and Clarke 2016, p. 1). Codes which share patterns of a central core idea are then aggregated into a theme (Ibid). For example, codes identified in the interview data such as 'lack of data centres', 'resource constraints', and 'shortage of data access devices' were aggregated into the theme 'inadequate infrastructure for privacy and data protection in The Gambia' (see chapter 3.2).

1.4.4 Ethics

As required by the research institution, an application to gain ethical approval was submitted to the Norwegian Agency for Shared Services in Education and Research and was approved. The thesis did not deal with sensitive information such as health information but only contained the opinions of key informants on the phenomenon of privacy and data protection in The Gambia. Prior to the interview, each participant was provided with a consent form (Annex 2) that had received approval by the Norwegian Agency. Participants were asked to read and sign the form if they were willing to participate. The form included details such as the study's aim, interview duration, confidentiality assurances for participants, and their right to refuse any question or withdraw from the interview at any stage. Information on the protection, security, storage, and access to the collected responses/data was also communicated to the participants.

The audio and transcript files were aggregated in anonymized folders and stored on a singular hardware system accessible only by the researcher. The data is stored for the duration of the research and until three months after the submission of the thesis. All research data (and metadata) stored on the hardware are thereafter deleted.

1.6 Literature Review

1.6.1. E-government Implementation

Chaffey (2009, p.189) defines e-government as the utilization of information communication technologies (ICT) for the delivering of government services to citizens. Chaffey (ibid) asserts that through e-government, national governments can employ ICT to offer improved, cost-effective, convenient, and efficient services. According to UNESCO, in order to achieve "good" governance, which they define as the exercise of power by various levels of government that is effective, honest, equitable, rights-respecting, transparent & accountable, the use of digital technologies is essential (UNESCO, 2005). They highlight that these electronic services further the empowerment of citizens through greater access to government information and ability to interact and participate in public affairs pursuant to the right to participate in public affairs as codified in Article 25 of the International Convention of Civil and Political Rights (ICCPR). Furthermore, UNESCO further highlights that electronic delivery of information and services not only enhances efficiency and quality but also promotes equitable access, benefiting both urban and rural populations through convenient channels such as the Internet, kiosks, integrated service centres, and mobile devices (UNESCO, 2005).

There are four types of e-government services. These first is Government-to-citizen (G2C) which encompasses the distribution of information to the public and provides fundamental citizen services, such as renewing licenses, obtaining birth/death/marriage certificates, and filing income taxes. Additionally, it offers citizen support for essential services such as education, healthcare, libraries, and similar amenities services (Solinthone & Rumyantseva, 2016, p. 2). G2C e-government services in The Gambia are the focus of this thesis. The second type is Government-to-business (G2B) transactions which encompass a range of services conducted between the government and the business sector. These services involve the distribution of policies, memos, rules, and regulations to facilitate business operations. Businesses can access a variety of services including obtaining up-to-date business information, downloading application forms, renewing licenses, registering businesses, acquiring permits, and fulfilling tax payments (Solinthone & Rumyantseva, 2016, p. 3). The

third type is Government-to-employee (G2E) services which encompass specialised offerings exclusively designed for government employees. They include provisions for human resource training and development aimed at enhancing the efficiency of bureaucratic operations and interactions with citizens on a daily basis (Solinthone & Rumyantseva, 2016, p. 3). While the final type is Government-to-government (G2G) services which occur on both domestic and international fronts. Domestically, they involve transactions between central/national and local governments, as well as between various departments, attached agencies, and bureaus. Internationally, G2G services serve as a tool for fostering international relations and diplomacy, facilitating interactions between governments (Solinthone & Rumyantseva 2016, p. 3).

While proving essential to governmental operations, the problem with e-government services is that it substantially increases the volume of records, storage, and processing of personally identifiable information by the government, which poses a great risk to individual's right to information privacy (Wu 2014, p. 150). For example, individuals who seek to be anonymous can be identified through corelation of big data sets, such as linking medical insurance records and voter registration records to identify confidential information about an individual (Shamsi & Khojaye 2018, p. 74). Government can also use personal information collected to track the activities of individuals without their consent (Ibid). The potential for information privacy violations has affected citizenry trust in e-government services manifesting in some reluctance to use them in spite of their usefulness. For instance, in the US, citizens expressed scepticism and mistrust towards e-government implementation, fearing potential invasion of privacy by the government (Belanger and Hiller, 2006). Other studies in developing countries such as Zimbabwe and Zambia have disclosed that citizens' acceptance and utilization of e-government services was affected by key factors including perceived lack of privacy, security, and trust in these services (Munyoka and Maharaj 2019, p. 7). Regardless, citizens largely do not have a choice but to interact with these services as they may be legally required to do so, such as in the use of e-government services to register for and pay taxes (Pina et al 2009, p. 20). Anonymity or pseudonymity is also often impossible if not illegal when dealing with government, as individuals usually have no choice but to provide personal information through these e-government services, at the risk of its users (Mayer-Schonberger & Lazer, 2007, p. 286). Thus, balancing the rapid implementation of e-government services and the need to guarantee individuals' right to information privacy has emerged as a pressing issue globally (Wu 2014, p. 150).

1.6.2. Information Privacy and Data Protection: Legal and Technical Perspective

Information privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others, and this right extends to personal information divulged in the use of e-government services (Westin 1967, p.7). Data protection, on the other hand, entails the regulation of the way organizations collect, store, manage, and disclose personal information (Bennett 2000, p. 33). Viewing data protection from a human rights perspective is important because in any civil society, privacy safeguards are a cornerstone of basic human rights (Coombe 2009, p. 395), and effective human rights centric data protection is a tool for the better protection of the right to information privacy. The integration of data protection with privacy rights highlights their inseparability, with each enhancing the effectiveness of the other (De Aguiar Borges 2023, p. 1788). Thus, the state has a special obligation to secure and protect the data of citizens as it creates the context and implements the legal provisions for the protection of user data pursuant to the right to information privacy (Pleger et al 2021, p. 1). Data protection primarily encompasses two aspects – the legal aspect, and the technical aspect also called 'technical data protection' (Ibid, p. 3). The legal aspect refers to the legal framework (e.g., laws, acts and regulations) dealing with the protection of data and information privacy. It also involves the enforcement and implementation of the legal framework (Ibid). This domain of data protection is mainly explored and determined by government administrations and politicians. The technical aspect, on the other hand, focuses on designing technology that ensures automated data processing is inherently compliant with the law (Ibid). It involves the use of technical measures implemented to protect stored or transmitted data from unwanted human, natural, accidental, or technical interference (Ibid). An example of such measures is the adoption of cookie management software or encryption technologies (Ibid). This domain is mainly explored by technicians handling technical aspects, such as cybersecurity or software engineering.

Regardless, the technical aspect can be influenced by the legal aspect as seen in Article 32 of the GDPR where it is stated that data controllers and processors are obliged to undertake "technical and organisational measures to guarantee the safeguard of personal data" (Council of Europe, 2018). Beyond law, the technical aspect of data protection can also be influenced by organisational factors such as ethical culture, availability of qualified human resources, and operational procedures (Pleger et al 2021, p. 3). Both aspects of data protection are, however, necessary for effective data protection and do directly affect the way e-government services

process data (Ibid). Given that laws and technical capacities vary between countries, independent and country-specific studies have been conducted to examine the existence and effectiveness of data protection measures within e-government operations. For example, Mutimukwe et al (2018) assessed the status of existing IPP practices in e-government in Rwanda, using international privacy and data protection principles as an assessment baseline. This study focused on actions by the e-government service providers, and found that the lack of adequate legislation, and gaps in some technical respects affect the protection of information privacy in e-government services in Rwanda (Ibid, p. 11). However, no similar studies exist on The Gambia, and this thesis seeks to create new knowledge by exploring the existence and efficacy of data protection measures in e-government services in The Gambia. While Mutimukwe et al. (2018) used principles of data protection as an assessment basis, this thesis goes further by incorporating recognized human rights standards for information privacy and data protection, integrating human rights theories into the analysis.

1.7 Theoretical Framework

This thesis utilises the "engineering for human rights" theoretical framework which advocates for the adoption of a human rights approach to the development and implementation of engineering projects (Chacon-Hurtado et al, 2023 p. 16). It argues that engineers should not only be technically proficient but also ethically conscious, integrating human rights principles into their work from the design, monitoring to evaluation, to ensure that their projects contribute positively to society while minimizing harm and upholding fundamental rights (Ibid, p. 16). This is because engineering projects often prioritize technological solutions to societal challenges rather than directly addressing human rights issues. However, these projects can inadvertently impact human rights and the environment. The framework encompasses three core duties for engineers which include taking actions to prevent harm (preventive approach), actions to remedy harm when it occurs (restorative approach), and actions to fulfil human rights (proactive approach) [ibid p. 16].

The preventive approach emphasizes the importance of engineers to mitigate any negative consequences on human rights or the environment that may arise from their projects. The goal is to prevent harm before it occurs or lessen its impact. The framework recommends the use of human rights impact assessments (HRIA) as a tool to identify potential negative impacts of a project in order to develop preventative measures (ibid, p. 16 and 17). The restorative approach in engineering involves engineers taking steps to rectify or directly confront instances of human

rights violations. An example is engineers utilizing geospatial imagery analysis to identify areas where mass human rights abuses are taking place in real-time. In essence, playing a role in investigative and remedial actions to address human rights violations, and contributing their technical expertise to promote accountability and justice (ibid, p. 18). The proactive approach in engineering involves engineers anticipating and addressing potential issues related to human rights during the development and implementation of technologies. For example, designers of new technologies, like autonomous vehicles, should ensure accessibility for people with disabilities, aligning with the Convention on the Rights of Persons with Disabilities (ibid, p. 18 and 19).

This theoretical framework is relevant to this study, which focuses on e-government services typically developed by software or computer engineers. These engineers design, develop, and distribute these information technology systems for the use of government agencies to provide essential services to citizens. As such, these engineers play an important role in the outcomes from the use of these e-government services, including human rights outcomes related to privacy and data protection. This thesis contributes to the theoretical discourse on "engineering of human rights" by emphasizing the government's role in ensuring that the core duties within this framework are met. The "engineering for human rights" framework acknowledges that while engineers have a duty to uphold, engineering objectives are, however, heavily influenced by predominant entities such as governments and businesses, but this is not discussed in detail within the framework (ibid, p. 8). This thesis explores this aspect by delineating the roles of government and engineers in integrating privacy and data protection measures that align with established human rights standards into the operations of e-government in The Gambia. Using the findings from the research, it proffers arguments as to who carries greater responsibility for the "engineering of human rights" in e-government implementation, and the extent to which each actor should be held accountable for identified gaps in information privacy protection in e-government in The Gambia.

Chapter 2: Information privacy and data protection- a human rights issue.

2.1 Introduction

This chapter delves into the complex intersection of privacy and data protection as fundamental human rights by exploring the evolving legal frameworks, and practical challenges surrounding these issues. By doing so, it will establish the human rights benchmark for information privacy and data protection, against which the operations of e-government services in The Gambia will be assessed. The chapter will also explore how the Gambia's obligations under the international human rights framework to protect information privacy, detailing how these obligations are reflected in its domestic laws and regulations.

2.2 Global Instruments for Information Privacy and Data Protection

The Universal Declaration on Human Rights (UDHR, 1948) provides for the right to privacy in Article 12 which states that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks". This provision has gone on to inspire an almost identical provision in the International Covenant on Civil and Political Rights (ICCPR) in Article 17 of the treaty.

From the reading of both articles, the right to privacy is considered both a positive and negative right. It is a negative right in that it provides individuals with protection from interference by others, including the government and private entities, ensuring that they are free from unwarranted intrusion into their personal lives (Human Rights Committee, 1988). Conversely, it is also a positive right because it entails the entitlement to certain actions or protections by authorities to uphold privacy, such as implementing laws and regulations to safeguard personal information, ensuring individuals have access to their data, and rectifying any inaccuracies (UN Human Rights Committee, 1988). Thus, while the negative aspect prevents unwanted intrusion, the positive aspect necessitates proactive measures to ensure privacy is respected and upheld by both state and non-state actors.

In General Comment 16, the UN Human Rights Committee, the independent treaty body for the ICCPR, stated that Article 17 mandates the legal establishment of fundamental data protection assurances in both the public and private sectors. In the committee's own words:

> "The competent public authorities should only be able to call for such information relating to an individual's private life the knowledge of which is essential in the interests of society as understood under the Covenant. [...] The gathering and holding of personal information on computers, databanks and other devices, whether by public authorities or private individuals and bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination". (UN Human Rights Committee, 1988)

This general comment outlined basic elements of privacy with regards to the protection of personal data pursuant to Article 17 of the ICCPR. From these elements scholars have developed some basic principles for data protection (Bygrave, 1998, p. 250). These include:

a) Fair collection: personal data should be gathered by fair and lawful means (i.e. the fair collection principle).
b) Data minimization: personal data collected, processed, and stored should be limited to what is necessary for the specific purposes for which it is being processed. This principle is designed to reduce the risk of excessive data collection (i.e. the minimization principle).
c) Quality collection: personal data should be accurate, complete and relevant in relation to the purposes for which they are processed (i.e. the data quality principle).
d) Regulated by law: personal data should be gathered for specified and lawful purposes and not processed in ways that are incompatible with those purposes (i.e. the purpose specification principle).
e) Restricted access: security measures should be implemented to protect personal data from unintended or unauthorized disclosure, destruction or modification (i.e. the security principle).

f) Transparency: Individuals have the right to know what personal data is stored in automatic data files, for what purposes it is used for, and who controls or may control their files (i.e. the transparency principle)
g) Individual participation: data subjects should be informed of, and given access to, data on them held by others, and be able to rectify these data if inaccurate or misleading (i.e. the individual participation principle).
h) Accountability: parties responsible for processing data on other persons should be accountable for complying with the above principles (i.e. the accountability principle).

Bygrave (1998, p. 253), however, expounds that while general comment 16 on Article 17 of the ICCPR lays down fundamental principles for safeguarding the right to privacy concerning personal data, there are certain crucial aspects absent in it. Bygrave (1998, p. 254) highlights, among other things, that the committee's comment regarding security measures focuses solely on the need to maintain the confidentiality of personal data, neglecting to explicitly address the importance of safeguarding against unauthorized alteration or destruction, ensuring data integrity, and ensuring that personal data are adequate, relevant, and not excessive in relation to their processing purposes. Furthermore, he pinpoints that there is no mention of special categories of data that may necessitate heightened protection, such as sensitive information like health or ethnicity (Ibid, p. 254).

These gaps have led to calls for an update to General Comment 16, which is yet to happen (UN Treaty Body Database, 2024). The American Civil Liberties Union explain that the General Comment 16 makes no reference to the internet and other emerging technologies (ACLU, 2014). Given that the General Comment was made in 1988 when internet technologies were still at its infancy, it is reasonable that the Comment would not address issues of privacy surrounding the use of internet technologies. However, the ACLU points out the oversight in foreseeing the evolution from traditional fixed-line telephone systems to widespread mobile telecommunications, the emergence of metadata, the intricate relationships between Internet companies, service providers, and governments underpinned by mandatory data-retention laws, and the extensive capabilities of states to monitor online activities through mechanisms such as social media tracking and IP address analysis (ACLU, 2014). This omission is notable, for example, as the U.N. Special Rapporteur on freedom of expression pointed out that metadata encompasses personal details about individuals, including their location, online activities, and records of emails and messages they exchange (UN Human Rights Council, 2013). This communication data is easily stored, accessed, and searched, with limited regulation governing

its disclosure and utilization by state authorities (UN Human Rights Council, 2013). Additionally, the rise of biometric data collection, including fingerprinting, facial recognition software, and DNA databases across jurisdictions, underscores the urgent need for a reassessment of General Comment 16 (ACLU, 2014).

The UN Special Rapporteur on the right to privacy,[1] Ana Brian Nougrères, also acknowledged the transformative impact of digital technologies on society and the consequent need for robust legal frameworks to protect individuals' personal data and privacy in this digital era (UN Human Rights Council, 2024). Among the potential privacy risks that exists in the digital age, according to the Special Rapporteur, are extensive data collection, surveillance, profiling, and the commodification of personal data by private entities. While the Special Rapporteur did not call for an update to General Comment 16, she did reiterate the importance of grounding data protection and privacy laws within the international human rights framework, with robust regulatory oversight mechanisms to enforce compliance with data protection laws and hold violators accountable (UN Human Rights Council, 2024). She stressed that "to safeguard their dignity, individuals must have sufficient means and mechanisms at their disposal to be able to assert their right to privacy" and that "the mere recognition of a legal standard on the right to personal data protection does not guarantee the effectiveness or enjoyment of that right without the existence of an accessible and effective protection system" (UN Human Rights Council, 2024). The Special Rapporteur further emphasized the necessity for states to implement a framework ensuring the protection of individuals' right to personal data, noting that this framework should enable data subjects to be informed about how their personal data is being processed; empower them to exert control over their data; and provide avenues for seeking redress, including reparation, restitution, or compensation, in case of a breach (UN Human Rights Council, 2024). There are no commentaries from the UN Human Rights Council and the Special Rapporteur on the right to privacy regarding issues of privacy and data protection in The Gambia.

2.3 The EU and Instruments for Information Privacy and Data Protection

Europe has some extensive treaties protecting the right to privacy and data protection. The right to respect for private life was guaranteed under Article 8 of the European Convention on

[1] The Special Rapporteur is mandated by the Human Rights Council to promote and protect the right to privacy by reviewing government policies and laws on the interception of digital communications and collection of personal data; Identifying actions that intrude on privacy without compelling justification; and Assisting governments in developing best practices to bring global surveillance under the rule of law among others

Human Rights and Fundamental Freedoms, hereinafter called the ECHR, which is similar in character to article 17 of the ICCPR, as it did not explicitly provide for the protection of personal data (ECHR, 1950). However, the European Court of Human Rights (ECtHR) has applied the 'living instrument doctrine', which is a doctrine that states that a Convention should be interpreted considering present-day circumstances (ECHR, 1978). This came about in the case of *Tyrer v. the United Kingdom*, which marked the first time the Court acknowledged the need for dynamic interpretation of the Convention's provisions to address evolving realities, challenges, and threats (ECHR, 1978). The court further reinforced this position in *Airey v. Ireland* in which it confirms that the rights outline in the Convention should not be deemed as exhaustive if they are to be "practical and effective, not theoretical and illusory" (ECHR, 1979). More specifically, with regards Article 8, the court stated in *Peck v United Kingdom* that 'private life' under this Article of the Convention "is a broad term not susceptible to exhaustive definition", as initially, personal data protection was closely linked to the right to private life (ECHR, 2003). As a result, the ECHR has continually expanded the boundaries of the right to private life and has interpreted various aspects of personal data protection with due respect to the 'living instrument doctrine'.

Even defining what constitutes personal data is ever expanding, and not only includes typical information like names or dates of birth. It extends to other data points that could potentially identify an individual, such as IP addresses, GPS data, or DNA profiles. For example, in *Benedik v. Slovenia*, the ECHR found that data on the subscribers' dynamic IP address constitute personal data since it could lead to the identification of an individual (ECHR, 2018). In another case of *Uzun v. Germany*, the ECHR acknowledged that GPS information is considered personal data and falls under Article 8 of the Convention, given that it may determine the locations and movements of a person in the public sphere. (ECHR, 2010). Unlike General Comment 16 on article 17 of the ICCPR, the ECHR has also interpreted article 8 of the Convention as having provided elevated protection to the processing of sensitive personal data, including health-related information, racial or ethnic origin, political opinions, religious beliefs, genetic and biometric data, and details about a person's sex life or sexual orientation due to its sensitive nature (see *Z v. Finland,* ECHR, 1997).

The ECHR through its judgements demonstrate the expansiveness of article 8 of the Convention to include all facets of private life, as well as protect all aspects of current and emerging types of data. Regardless, the Council of Europe, has provided a more comprehensive articulation of the right to personal data protection through Convention no. 108, known as the

Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, 2018). Convention no. 108 stands out as the inaugural international treaty to define personal data and delineate fundamental principles of data processing. With international law still facing challenges in protecting personal data due to the lack of a universal agreement on its scope, there are calls for a global treaty on data protection, with Convention no. 108 seen as a good starting point, as it's the only binding international treaty on this topic and is open to countries outside Europe (Buttarelli, 2016). Some argue it should become a global treaty under the UN to provide uniform data protection worldwide (Greenleaf, 2018). To keep up with changes brought by the digital age, Convention no. 108 has been updated through a protocol to make it stronger. This update was in relation to the protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, 2018).

In the EU, the right to personal data protection was addressed in various documents like Directive 95/46/EC and the Charter of Fundamental Rights. The most recent regulation, General Data Protection Regulations (GDPR), also focuses on this, and took full legal effect across the European Union (EU) and, subsequently, the European Economic Area (EEA) which comprises of thirty states. (Council of Europe, 2018). The GDPR is a vast and intricate data protection law, comprising 99 articles across 88 pages. It establishes a comprehensive legal structure for safeguarding personal data of data subjects and promotes responsible data processing for various legitimate purposes (GDPR, Regulation 2016/679). To achieve this, the GDPR outlines the following key provisions:

Article(s)	**Subject Matter**
3	*Territorial scope of the GDPR*. The GDPR has an expanded territorial scope, applying to establishments of controllers or processors within the EU, as well as to non-EU organizations that monitor the behaviour of individuals in the EU or intend to offer goods or services to individuals within the EU.
4	*Definitions* (e.g. “personal data,” “genetic data,” and “data concerning health”)
5	*Principles relating to processing of personal data*. These provisions include provisions of fair collection, accountability and transparency and all other principles as outlined in Bygrave, 1998, p. 250
6	Legal bases for processing personal data
7	Conditions for consent where consent is used as a lawful basis
9	*Processing of special categories of personal data* (i.e. sensitive data) and conditions under which such data may be processed – see in particular Art. 9(2)(j) (processing necessary for scientific research purposes)
13	Information to be provided where personal data are collected from the data subject

14	Information to be provided where personal data have not been obtained from the data subject
22	Data subject rights regarding automated individual decision-making, including profiling [note: this may not be derogated from under Article 89]
25	*Data protection by design*. necessitates data controllers to incorporate suitable technical and organizational measures that align with data protection principles, like data minimization, both during the determination of processing methods and during the processing itself. By default, on the hand, personal data should not be made accessible to an unlimited number of individuals without the individual's active involvement.
35	*Data protection impact assessments.* When data processing, especially involving new technologies, is anticipated to pose a significant risk to the rights and freedoms of data subjects, the controller must conduct a prior assessment of the potential impact of the processing on personal data protection, known as a "data protection impact assessment".
37-39	*Data Protection Officers (DPOs*). The GDPR mandates internal record-keeping obligations for organizations and requires the appointment of a "Data Protection Officer" (DPO), which is compulsory for controllers and processors that are public authorities or whose core activities involve data processing, among other criteria.
40	Codes of conduct
44-49	Transfers of personal data to third countries or international organizations
89	Safeguards and derogations relating to processing for scientific research purposes

The GDPR holds significant importance in the global movement to protect data on both national and international levels for several reasons. It establishes a robust set of data protection standards, serving as a model for other countries and regions in developing their own data protection laws. Furthermore, its broad territorial scope that extends beyond the EU, impacting organizations worldwide that process personal data of EU residents, has prompted companies operating outside the EU to comply with GDPR requirements, thereby enhancing data protection best practices internationally.

While The Gambia is neither a party to the GDPR nor the Convention, it is a party to the ICCPR (ratified in 1979) and is thus under an obligation to protect the privacy rights of its citizens, including information privacy rights. The Gambia is, however, situated in a region where data protection and information privacy measures are still evolving and trailing behind other parts of the world, such as Europe (Reuters, 2018).

2.4 African Instruments for Information Privacy and Data Protection

The African Charter on Human and People's rights, hereinafter referred to as the Charter, for example, does not contain any provisions on the respect and protection of privacy rights, particularly information privacy (Singh, & Power, 2019 p. 207). The Gambia is a party to this charter having ratified it in 1983 (ACHPR, 1981). It is important to note that the Charter does

provide for bodily privacy which focuses on safeguarding individuals' physical integrity from intrusive measures in article 4 (ACHPR, 1981). To understand, however, why information privacy is not catered for in the Charter, privacy developments in Africa should be viewed in the context of a cultural emphasis on collectivism, exemplified by the South African proverb "umuntu ngumuntu ngabantu abanye" (a person is a person through other persons), commonly known as Ubuntu (Kamwangamalu, 1999). This cultural framework prioritizes communalism, interdependence, and mutual care, which some have argued may have influenced the interpretation of the right to privacy in African states, including its absence in the Charter (Olinger et al, 2007).

So far, the African Court on Human and Peoples' Rights (ACtHPR) and the African Commission on Human and Peoples' Rights (ACmHPR) have not extensively developed jurisprudence regarding the right to privacy in Africa (Ayalew, 2022). The ACmHPR, which is tasked with promoting and protecting human rights by interpreting the African Charter and considering individual complaints (ACHPR, 1987), received a draft resolution in 2019 on the right to privacy, endorsed by the NGO Forum, highlighting privacy's importance for various rights, and suggesting the inclusion of privacy and digital rights in the Special Rapporteur's mandate (Legal Resources Centre, 2018). The draft resolution was however, not formally adopted by the Commission, but the text of the draft resolution is used for informative purposes (Singh, & Power, 2019 p. 210). Furthermore, the African Commission has recently reviewed and ratified the updated 2002 Declaration of Principles on Freedom of Expression and Access to Information in Africa, which incorporates substantial provisions concerning the right to privacy, albeit being a non-binding instrument (Ibid, p. 210).

Some have argued that, in spite of the lack of an express provision for the right to privacy in the Charter, both the ACmHPR and ACtHPR can give life to the right to privacy by reading the right into other provisions of the Charter such as the right to dignity, drawing inspiration from landmark Indian Supreme Court decision in *Puttaswamy* (Ibid, p. 213). The main issue before the Supreme Court was whether the right to privacy is a constitutional right in India, despite its absence in the explicit text. Specifically, the Court had to determine if the right to privacy could be inferred from Article 21 of the Constitution, which guarantees the protection of life and personal liberty (Ibid, p. 213). The Court acknowledged the significance of privacy in upholding the rights to life and dignity and dismissed the notion that acknowledging the right to privacy necessitated a constitutional amendment, reasoning that it is inherently tied to the liberties already guaranteed in the Indian Constitution (Ibid, p. 214). By affirming that the right

to privacy is integral to human dignity, the Court concluded that recognizing it as a constitutional entitlement did not entail creating a new fundamental right (Ibid, p.214). The ACmHPR had previously read non-prescribed rights into existing ones in the Charter as seen in the case of *Social and Economic Rights Action Centre and Another (SERAC) v Nigeria* where the ACmHPR read the non-prescribed right to food into the statutorily provided rights to life, health and economic, social and cultural development (Ibid, p. 212; also see ACmHPR, 2001).

There are however two African regional treaties that explicitly contain the right to privacy. The first is the African Charter on the Rights and Welfare of the Child (ACRWC, 1990) which The Gambia is also a party to having ratified it in December 2000 (AU, 2023). The ACRWC provides in Article 10 that:

> "No child shall be subject to arbitrary or unlawful interference with his privacy, family home or correspondence, or to the attacks upon his honour or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks." (ACRWC, 1990)

The ACRWC however has limited application as the rights contained therein only apply to children which it describes as 'every human being below the age of 18 years' (ACRWC, 1990 Article. 2). The African Union has also promulgated a convention on Cyber Security and Personal Data Protection (also referred to as the Malabo Convention) with the aim of advancing the 'Information Society' while safeguarding citizens' privacy and ensuring the free flow of information. The convention underscores the commitment of each state party to establish a legal framework that strengthens fundamental rights and freedoms, particularly the protection of personal data, and to prosecute privacy violations while upholding the principle of data flow (Article 8.1, the AU Data Protection Convention, 2014).

The Malabo Convention closely mirrors several standards and principles outlined in the GDPR, and contains similar to identical provisions therein (Ayalew, 2023). The Convention includes data protection principles, the rights of data subjects, data processing restrictions, cross border data transfer, security measures, data protection authorities, international co-operation, enforcement and remedies (African Union, 2024). One key difference from the GDPR, however, is that the Malabo Convention applies territorially, covering data processing activities within the territories of State parties, regardless of whether they are automated or not, while the GDPR has an extra-territorial reach, applying to data processing activities conducted by

establishments within the European Union, even if the processing occurs outside the Union (Ayalew, 2023). Furthermore, the Malabo Convention lacks clarity regarding its applicability to data processors or controllers outside the continent, a matter addressed by the GDPR when processing activities relate to offering goods or services to individuals in the EU or monitoring their behaviour within the Union (Ayalew, 2023). The Malabo Convention, which requires ratification by fifteen member states to become effective according to Article 36, came into force in June of 2023, after it obtained the required amount of state ratifications (Alt-advisory, 2023). The Gambia is one of the African countries that has recently ratified this convention, after it had indicated its intention to do so by signing it in 2022 (Alt-advisory, 2023). The Gambia is also party to the Economic Community of West African States (ECOWAS) Supplementary Act on Data Protection, which seeks to achieve the same goals as the Malabo Convention. This sub-regional treaty only applies to West African ECOWAS member states and has been in force since 2010 (ECOWAS, 2010). Compliance with both instruments would primarily require the enactment of comprehensive data protection laws and regulations that reflect the principles and provisions outlined in the Malabo Convention; and the Creation of a Data Protection Authority tasked with overseeing compliance with data protection laws, handling complaints from data subjects, and promoting awareness of data protection rights and responsibilities (African Union, 2014; ECOWAS, 2010). Orji (2017) contends that there is presently a lack of an effective regional mechanism to ensure member states' compliance with the obligations outlined in the ECOWAS Supplementary Act. Part of this argument is that there is an inapplicability of sanctions against ECOWAS Member States that have not implemented their obligations under the ECOWAS Data Protection Act (Orji, 2017). This absence of sanctions results in a scenario where compliance cannot be assured.

2.5 Legal instruments in The Gambia for Information Privacy and Data Protection

The Gambia is a dualist state, requiring adopted international treaties to be domesticated into national law by parliament for the provisions of those treaties to be applicable in The Gambia (Constitution of The Gambia, 1997, Article. 7). A prime example of this, and one that is the focus of this thesis, is article 23 of the 1997 Constitution of The Gambia, hereinafter called the Constitution, which provides for the right to privacy by stating that individuals shall not be subject to ‘interference’ with privacy of their home, correspondence, and communications, except when such interference is lawful and necessary (Constitution of The Gambia, 1997). This provision not only provides for the right to privacy in general, but also attempts to protect

the right to information privacy in particular by including the protection of correspondences and communications. As correspondences and communications frequently involve personal information, such as names, addresses, financial details, and other communication content, it is vital that that right to privacy encapsulates these in order to protect information privacy. However, it is worth assessing if this constitutional provision is sufficient to protect information privacy rights, and by extension protect data, in The Gambia.

The provisions of the Constitution are similar to the provisions contained in Article 17 of the ICCPR which also purports to protect information privacy, and The Gambia is one of 52 African states to include the right to privacy in their current Constitutions (Singh, & Power, 2019 p. 204) all of which are party to the ICCPR (UN Treaty Body Database, 2024). The previous two Constitutions of The Gambia i.e. The 1965 Independence Constitution, and the 1970 Republican Constitution contain no reference to the protection of the right to information privacy, such as correspondences and communications (Law-hub Gambia, 1965 & 1970). Both Constitutions, however, came into force before The Gambia adopted the ICCPR in 1979 (UN Treaty Body Database, 2024). The 1997 Constitution, on the other hand, which came into force after The Gambia adopted the ICCPR, contains provisions that protect information privacy rights- further confirming the influence of the ICCPR on the national protection of privacy. It provides in Article 23 that:

> "No person shall be subject to interference with the privacy of his or her home, correspondence or communications save as is in accordance with law and is necessary in a democratic society in the interests of national security, public safety of the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime or for the protection of the rights and freedoms of others." (Constitution of The Gambia, 1996)

There are no known reported cases of Gambian Courts providing a detailed interpretation of the right to privacy and what it encompasses, as provided for in the Constitution (Data-Guidance, 2023). This creates a gap in knowledge on how this right, particularly relating to information privacy, is to be protected and respected. For example, article 23 of the Constitution does not state on whom the responsibility lies to protect the right to privacy (i.e. either or both public or private authorities. Furthermore, the provision in article 23 calls for no 'interference' into the privacy of individuals in The Gambia, implying that this is a negative right requiring no action from the government or any other responsible authority. However, as

detailed in Chapter 2.2, the right to information privacy requires both the negative action of non-interference and positive action by both public and private authorities that handle personal information. General Comment 16 of article 17 of the ICCPR clearly explains that States must take 'measures' to prevent unauthorized access, processing, and use of personal information to safeguard individuals' privacy (General Comment 16, 1988).

Without a current court interpretation of article 23 of the Constitution, however, it can be argued that relying on this article to protect the right to information privacy, and by extension protect data, may prove challenging. The current status regarding the application of General Comment 16, which provides a comprehensive explanation of the application and implementation of the right to privacy under the ICCPR (General Comment 16, 1988), remains unknown in The Gambia. General Comments tend to serve as interpretive statements, rather than as binding instruments, so it is usually up to states to decide whether or not they are applied accordingly (Keller & Grover, 2012 p. 117). Some states have treated these comments as 'authoritative interpretations' of treaty norms, while other states have treated them as 'not deserving of being accorded any particular weight in legal settings' (Ibid, p. 118). It cannot be affirmed that the interpretation of the right to privacy in General Comment 16, which encompasses privacy of information data, would be adopted by Gambian courts in the interpretation and enforcement of Article 23 of the Constitution.

The one other legislation that provides for the right to information privacy is the Children's Act of The Gambia (2005), which was inspired by the ACRWC and the Convention on the Rights of the child (CRC), both of which contain the right to privacy for children (CRC, 1989, article 16; also see ACRWC, 1990 Article 10). But as with the ACRWC, and the CRC, the provisions of the Children's Act on the right to privacy has limited application to only persons under the age of 18 (Children's Act, 2005, Article 2). This is problematic as the majority of e-government services, such as those involved in the registration of voters, production of national I.Ds and driver's licences are used by adults. The Children's Act provides that "no child shall be subject to arbitrary or unlawful interference with his or her privacy, family life, home, correspondence, or to attacks on his or her honour or reputation" (Ibid, Article 10). This provision runs into similar problems as Article 23 of the Constitution with regards its wordings of 'no interference', and a lack of a detailed explanation on who the duty falls to protect this right, and more importantly, how they are to go about protecting this right (Ibid, Article 10).

These important details could be captured in a legally binding instrument such as the GDPR in the EU. The Gambia, however, lacks a specific legislation addressing issues of information privacy, and data protection concerns despite adopting several international, regional, and sub-regional instruments that place an obligation on the Gambia to implement a data protection legislation (Data-Guidance, 2023). A Personal Data Protection and Privacy Bill, as of December 2023, has been drafted, undergone review, finalization, and submission for Cabinet approval. Upon endorsement, the bill will proceed for parliamentary approval (State of The Nation Address, 2023 p.66). Nevertheless, it remains uncertain when this Bill, which has not been publicly available as of March 2024, will be enacted into law, if it will be enacted at all. Prior to the conception of this Bill, the Public Utilities Regulation Authority, in 2019, proposed a Data Protection and Privacy Policy (GMCSIRT, 2019), and it is this policy that has inspired the development of a potential privacy and data protection law in The Gambia, as it clearly states that:

> "The purpose of this policy is to lay the foundations of institutional and legal framework for data protection and privacy that will give effect to Section 23 of the Constitution of The Republic of The Gambia and to express the commitment of the Government of The Gambia to ensure the protection of personal data and associated rights of individuals, and in particular the right to privacy." (Ibid, p. 3)

The policy, which reflects developments and international best practices as captured in the Malabo Convention and the GDPR, contains among other things, the principles of data protection, special categories of data, protection by design, rights of data subjects, transborder flows of personal data, and establishment of a data authority (Ibid, 2019). As a foundational policy document, however, the Data Protection and Privacy Policy lacks the force of law, and not enforceable for the protection of data and information privacy rights (Data-Guidance, 2023).

Chapter 3: Findings on e-government services in The Gambia.

3.1 Introduction

This chapter embarks on a comprehensive exploration of the existence of privacy and data protection mechanisms within the operations of e-government services in The Gambia. Utilizing data from key informant interviews, which has been aggregated into themes and presented as sub-headings, this chapter aims to depict the realities of e-government implementation in The Gambia, focusing on information privacy and data protection concerns. The e-government services explored in this chapter include the Semlex ID Card and Passport system, the National Digital Health system, National Birth Registration system, and the Digital Car Identification system (See Chapter 1.1).

3.2 Inadequate framework and inadequate infrastructure for privacy and data protection in The Gambia

The implementation of e-government in The Gambia is marked by a conspicuous absence of robust privacy and data protection mechanisms, particularly evident in the lack of enforceable legislation governing the privacy of personal information and data protection. Expert 5 emphasized the critical need for comprehensive legislation and a strong enforcement mechanism, stating that "*The Gambia currently lacks the necessary legislation and regulations to protect information privacy rights*". Expert 5 further asserted that apart from legislation, The Gambia needs a strong enforcement mechanism, and a strong enforcement regime. This includes the establishment of a Data Commission and the appointment of Data Protection Officers to supervise the implementation of any data protection and information privacy laws that may be passed, and exercise regulatory oversight.

This position highlights the importance of effective enforcement alongside legislative measures to ensure meaningful protection of information privacy and personal data. Without effective enforcement, any legislative efforts risk languishing as mere symbolic gestures rather than actionable solutions (Expert 5). There are, however, scepticisms about the government's ability to implement any potential data protection framework, as Expert 4 argued that the effectiveness of the Data Protection and Privacy Policy of 2019, was undermined by governmental apathy towards its implementation, leading to the noticeable effects of a non-existent legislative framework for information privacy and data protection (Expert 4). This reinforces the position of Expert 5 that enforcement is just as important as the existence of an

adequate legal and regulatory framework for privacy and data protection within e-government services in The Gambia.

Expert 1 provided insights into legislative developments for information privacy and data protection, noting the approval of the Personal Data Protection and Privacy Bill by the Gambian cabinet, but stating that the Bill is still awaiting parliamentary ratification, with no stipulated timeline as to when this Bill will be debated by parliament. Additionally, Expert 1 underscored the necessity of enhancing physical and digital infrastructure to bolster data protection measures, stating that the government has to work on the physical and digital infrastructure to ensure better data protection and allocate adequate resources for this. Expert 1 explains that:

> *"we currently struggle with the tangible elements such as data centres, servers, networking equipment, and facilities where data is stored, processed, and transmitted. Without adequate physical infrastructure, data may be vulnerable to risks such as unauthorized access, theft, or damage. Therefore, strengthening physical infrastructure will involve investing in secure facilities, implementing access controls, and adopting best practices for data storage and management."*

Furthermore, allocating adequate resources is essential to support these infrastructure improvements and ensure their sustainability. This includes financial resources for procurement, deployment, and maintenance of hardware and software solutions, as well as human resources for managing and overseeing data protection initiatives. Expert 2 echoed this position by citing an example within the implementation of the digital health registry:

> "*The challenge is, we have encountered resource constraints with regards devices that can grant access rights to health officials for the national health database. So, what you end up creating is a situation where people are sharing access credentials, or access devices such as tablets to use the database. We know this is wrong as there are risks associated with the data, but this continues to be a challenge*" (Expert 2)

This example highlights that resource constraints in e-government implementation, such as a shortage of devices granting access rights, can lead to security vulnerabilities that may pose a threat to the privacy and data protection rights of individuals whose data is registered in these e-government services.

3.3 Lack of transparency and accountability in e-government service implementation

There exists a lack of transparency on how data is processed and stored. Expert 5 articulated deep-seated concerns on transparency relating to the collecting, processing and storage of data within some e-government systems in the country, and vividly illustrated this through the example of the digitization of birth certificate registration in The Gambia. Expert 5 recounted reluctance to participate in a call for all members of the public to register their births in the new digital birth registration system.

"When my wife told me she wants to take the kids for digital birth registration I refused because I did not know how they were going to store the information. When the kids were born at the hospital some years ago, their birth information had already been collected, using non digital means, by the same government and by the same healthcare system. We're not even sure how that information is stored or processed. And yet, they still want everyone to come back and do another birth registration to collect information that nobody knows how they store or use. I basically couldn't agree to that." (Expert 5)

This shows that a lack of clarity regarding the need for a new data collection exercise using this new digitised system, and a lack of clarity on the data processing and storage methods, inspired some scepticism among citizens, undermining their willingness to engage with these e-government services. There has also been a lack of accountability within the implementation of e-government projects in The Gambia. One of these projects is the digitisation of aluminium number plates to provide for QR codes for licensed cars. These QR codes which contained the personal information of the car owners, were contractually meant to be encrypted and be only readable by authorised officials with authorised devices, such as the Police. Through an investigation, Expert 3 found that the QR Codes on cars that had these digitised aluminium number plates, could be readable by any smartphone and would thus reveal the personal information of car owners to anybody with a smartphone. Expert 3 argued that this was in violation of the terms of the contract between the government and the private company that produced these QR codes stating, "*I read the contract for the supply of these number plates, and the terms with regards encryption are not being met, and I had raised this issue with the relevant authorities a few years ago, and until now this defect has not been corrected*" (Expert 3). This breach of contract, and the government's failure and inaction to resolve the issue of defective aluminium number plates that could expose personal information of car owners in

The Gambia, highlights a reluctance/ inability on the government's side to hold data processors accountable for breaching the privacy of users' data.

3.4 Non-adherence to the principle of data minimisation in The Gambia

The principle of data minimisation, according to expert 4, is a cornerstone of data protection and privacy, and advocates for the collection and retention of only the minimum amount of personal data necessary for a specific purpose. However, expert insights reveal significant shortcomings in adherence to this principle within The Gambia's e-government systems. Expert 4 highlighted the failure to implement data minimisation practices in everyday e-government processes, such as passport renewals at the Gambia's Immigration Department, which currently utilises the Semlex biometric systems to produce national passports and ID cards for citizens. Expert 4 explained that:

"*The Immigration department produces both the passport and the national ID Card, but even if you had already provided personal information to get a passport, you need to submit the same information all over again when applying for an ID Card. And this information had already been collected by the same department. And if you have to renew either document, you have to provide the same personal information such as your name, date of birth, all over again in a new application form*".

The expectation according to Expert 4 is that their previously collected personal data by the immigration department using a singular system (Semlex) would be accessible by them to renew documents they have produced or to produce similar documents without the need for new redundant data submission and collection. This inefficiency also raises concerns about data management practices within The Gambia's Immigration department and accessibility of data within the Semlex Biometric systems used by the Immigration department. Expert 5 who has similar experiences with the Gambian immigration department re-echoes this position by asking "*who says the information on the ID card cannot be used to produce my passport. Why do you need to screen me to get an ID card, and then screen me again to get a passport*? *And why do I have to produce the same information again when I want to renew my national documents*?" This highlights the perceived absurdity of the e-government operations which are expected to be efficient in its data management.

Furthermore, Expert 3 raised concerns regarding the prevalence of physical paper forms across e-government systems by pointing out the inherent vulnerabilities of such practices, emphasizing that physical forms can be easily accessed and manipulated by unauthorized

individuals. Expert 3 remarked that "*the way that data is collected is mostly still physical, that is, on physical paper forms. And anybody who has access to those papers has access to your personal information. We should move towards digital forms on all e-government systems, where they are actually a lot more secure.*" Expert 2 reinforced this by highlighting the transition to smart paper forms within the Ministry of Health in The Gambia, stating that while the form may be technologically advanced, the underlying process remains manual requiring the filling of paper forms, with the difference being that smart paper is machine readable with the data transferrable into digital form by just scanning, as opposed to using data entry personnel. While Expert 2 confirmed that the smart paper forms used by the Ministry of Health are archived, it is unclear where the paper forms used in other e-government services are stored after the information contained are entered into the e-government digital systems. The continuation of manual physical paper processes thus poses significant security risks, as anyone with access to these physical forms can potentially compromise sensitive personal information. The juxtaposition of advanced technology with manual data entry methods underscores the persistence of outdated practices within e-government systems in The Gambia.

3.5 Improved data-sharing within government as a goal of e-government

The Gambian government has stated that it is actively pursuing the integration of e-government systems to transition the majority of its government-to-citizen services into digital platforms, with the aim of enhancing access to essential public services for its citizens. However, there is a potential benefit for the government in implementing these digitised services, with associated risks for users. According to Expert 5, the implementation of e-government services plays an important role in enhancing the data sharing capabilities within the government i.e. among government ministries and departments.

Expert 1 explained that *"there is currently no collaboration in terms of how the ministries share data with each other, and public servants working in government departments experience difficulty accessing information from other departments. So, the whole idea is to improve the data sharing ability within the government."* This perspective suggests that the Gambian government aims to achieve vertical integration in e-government service implementation, wherein government services are interconnected, and transactions with one level of government are directly communicated to others. Expert 4 expressed scepticism about the government's ability to achieve this goal due to the disjointed approach to e-government implementation in The Gambia. This disjointedness arises from independent digitization efforts by various government institutions without coordination among themselves. Expert 4

emphasized that there needs to be a coordinated effort to ensure interoperability and data sharing among e-government systems in order to achieve vertical integration, highlighting the absence of such coordination presently. Expert 4 however highlighted that with vertical integration comes "*a significant increase in the volume and scope of data exchanges, and without adequate privacy and data protection measures in place, this increased data sharing raises serious concerns regarding the security, and confidentiality of our sensitive personal information*." Expert 4 concluded that with increased data sharing within government "*users would need to know who could be potentially viewing their personal information*".

The importance of data sharing capabilities within e-government systems in The Gambia extends beyond domestic service provision and into fulfilling international data sharing obligations. Expert 2 highlighted The Gambia's commitment as a party to the International Health Regulations (IHR) and its obligation to share health data with the World Health Organization (WHO) in the event of specific diseases or potential public health emergencies. According to Expert 2, *"the country is mandated to report its health indicators to their various international partners, and so what happens is that once all the data is generated on reporting formats on the digital health registry, the Ministry of Health then reports to all its partners on the 15th of every month."* This example captures the vital role of e-government services in facilitating timely and accurate data sharing and reporting to international entities, ensuring compliance with global health regulations and fostering collaborative responses to health challenges. It also shows that increased data sharing capabilities can be a positive development, but with the associated risks.

Chapter 4: Discussion of findings

The findings reveal that the information privacy and data protection mechanisms within e-government services in The Gambia are inadequate and fail to meet the standards established in human rights instruments. This discussion applies the "engineering for human rights" (EFHR) framework to highlight the shortcomings and provide a comprehensive understanding of the issues. As e-government systems are products of computer/ software engineering, this theory is apt for this discussion. While the framework focuses on engineers, this discussion explores the role of the government in "engineering for human rights" delineating the roles and accountabilities of both parties in a human rights centric e-government implementation. The framework stipulates that integrating human rights into engineering projects, such as e-government services, necessitates implementing three approaches: the preventive approach, which involves anticipating and mitigating potential negative impacts on human rights; the restorative approach, which requires taking actions to address and remedy any violations; and the proactive approach, which involves actively working to fulfil human rights through engineering projects (Chacon-Hurtado et al, 2023 p. 16).

The government and the private sector developers of e-government services (i.e. the engineers) have failed to adopt these approaches in the implementation of e-government services in The Gambia resulting in them failing to meet recognised standards for human rights. Firstly, there is an absence of a detailed legal framework for privacy and data protection in The Gambia, within which e-government services would operate. The findings show that several e-government services in The Gambia have and continue to collect personal data of individuals en mass, but the processes of collection, processing, and storage are not regulated by an information privacy right respecting law. This goes against international best practice for information privacy and data protection, and also against The Gambia's international obligations. The Gambia ratified the ICCPR in 1979 (OHCHR, 2024), and domesticated the rights granting provisions in the 1997 Constitution, including the right to privacy (Constitute-Project, 1997). The UN Human Rights Committee had provided in General Comment 16 on the right to privacy that "the gathering and holding of personal information on computers, databanks and other devices, whether by public authorities or private individuals and bodies, must be regulated by law" (UN Human Rights Committee, 1988). The Gambia is also party to the Malabo Convention and the ECOWAS Supplementary Act on Data Protection, both of which require that state parties enact comprehensive data protection laws and regulations that reflect the provisions of these instruments in order to be in compliance (African Union, 2014;

ECOWAS, 2010). The creation of a legal framework acts as a preventive approach as it establishes the information privacy rights of users, and obligations of data processors. This allows processors to be aware of actions within the operations of e-government services that may constitute violations of information privacy rights, thus adopting measures to avoid them. Engineers under the EFHR framework are also obligated to carry out a human rights impact assessment as a preventive measure, and in the case of e-government implementation, this would be a in the form of a privacy and data protection impact assessment to mitigate potential negative impacts particularly on user's data. However, it can be argued that this is in fact the responsibility of The Gambian government. In 2022, the Kenyan government was halted, by Court decision, from rolling out a digital ID system after it had failed to carry out a data protection impact assessment (DPIA). The Court held that the duty to conduct a DPIA rested on the State pursuant to its constitutional duty to respect the right to privacy (Okeyo, 2022). Drawing from this case it can be said that a greater responsibility for this preventive measure lies on the Gambian government, in accordance with its duties under the provisions of the Constitution and duties under the international treaties it has adopted. Engineers do have a role to play in these DPIAs as they have a greater understanding of the nature of the technology being deployed for e-governance services and can therefore better identify potential risks. However, the duty is on government to initiate this process. Okeyo (2022, p.1) further argues that DPIAs can be used by States with no data protection laws to ensure that privacy rights are respected in the deployment of technology. There is however no evidence that DPIAs are carried out before the implementation of e-government services in The Gambia.

While The Gambia has demonstrated some intent to be adherent to best practices of information privacy and data protection by signing data protection treaties, its failure to enact domestic law that provides for this adherence has a troubling legal effect. This is thanks to the legal principle of "no punishment without law" encapsulated in Article 24 (5) of the Gambian Constitution which states that "no person shall be charged with or held to be guilty of a criminal offence on account of any act or omission which did not at the time it took place constitute such an offence" (Constitute-Project, 1997). This constitutional provision reflects Article 15 of the ICCPR, and Article 7 of the ECHR which provide for the same principle. The effect of this is that in the event of a violation of information privacy and data protection rights, individuals, and institutions responsible for such violation cannot be held liable for the violation, and victims are unable to seek reparations. This situation also creates an environment where a restorative approach to EFHR is unfeasible as there are no laws catering to restitution, making

it futile for engineers to engage in restorative duties including participating in forensic investigations to uncover human rights violations, as these investigations are unlikely to yield restitution due to a lack of restitutive law. This situation is also contrary to the principle of accountability in data protection which requires that persons responsible for processing data on other persons should be accountable for complying (or failing to comply) with the core principles of data protection (Bygrave, 1998). Thus, having clear and enforceable data protection laws provides legal certainty for individuals, businesses, and government agencies on data rights of individuals and obligations of data processors and authorities towards those rights. Furthermore, The Gambia being a dualist state also makes it impossible for victims of information privacy violations to invoke protections by international statutes such as the ICCPR, and the Malabo Convention that The Gambia is a party to, as these statutes are not directly applicable in the courts of The Gambia (Article 7, Constitute-Project, 1997).

Another effect of the absence of domestic legal protections is the non-establishment of effective enforcement mechanisms for information privacy and data protection. As the UN Special Rapporteur on Privacy had stated "the mere recognition of a legal standard on the right to personal data protection does not guarantee the effectiveness or enjoyment of that right without the existence of an accessible and effective protection system" (UN Human Rights Council, 2024). The establishment of an enforcement mechanism usually includes an independent national data protection authority tasked with monitoring and supervising, through investigative and corrective powers, the implementation of data protection laws. Additionally, the authority provides guidance on data protection matters and addresses complaints alleging breaches of the law (European Commission, 2024). Enforcement mechanisms are usually established in law/regulation as seen in Article 51 of the GDPR which provides that "each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation…" (European Union, 2016). Ghana, a member state to the ECOWAS supplementary Act, just as The Gambia, also established a national data protection authority (DPA) in its Data Protection Act to enforce and monitor compliance with the provisions of the Act (NITA, 2012, Article 1). These enforcement mechanisms are thus essential to the proactive approach in EFHR which requires that engineers design systems to fulfil human rights from the outset. These mechanisms monitor and ensure that standards for information privacy and data protection set for goods and services are met by engineers, thus compelling them to fulfil their proactive duty under the framework.

This research however finds that enforcement mechanisms while essential, are absent, in the operations of e-government services in The Gambia, and while an enforcement mechanism can be created via the mandate of law, the existence of such legal provisions do not necessarily guarantee that an enforcement mechanism would be effective (Popiel & Schwartz-Henderson, 2022 p. 14 & 15). For example, DPAs in Low-to-middle income countries, even after establishment face barriers to achieving regulatory compliance, particularly significant resource constraints (both financial and human) that limit their ability to perform their mandate(s) of data protection enforcement (Ibid, p. 17). This problem is caused by government prioritizing other areas for funding due to limited finances or simply a lack of political will (Ibid, p. 18; also see Pisa et al, 2021). The research findings already show resource constraints affecting the operation of e-government services in The Gambia, exemplified by the lack of adequate access devices such as tablets for health workers using the digital health registry, leading to the sharing of access credentials and devices. With The Gambia being a low-to-middle income country, and with the government already struggling to allocate adequate resources for the operation of e-government services, it is possible that any data protection enforcement mechanism established would struggle to gain the necessary resources to function effectively.

The absence of comprehensive legislation regarding information privacy and data protection, compounded by a lack of effective enforcement mechanisms in The Gambia, results in widespread infringement upon data rights and principles, notably in the implementation of e-government services. Research findings indicate a breach not only of the fundamental principle that data should be governed by law but also of key principles such as data minimization, restricted access, transparency, and accountability in the operation of e-government services within the country. These breaches are not only in contravention of global best practices for data protection as contained in international instruments such as the ICCPR and the GDPR but also in contravention of The Gambia's obligations under the ICCPR, Malabo Convention, and the ECOWAS Supplementary Act on Data Protection. The occurrence of these breaches has diminished trust in the utilization of e-government services among the key informants. This decline in trust observed among the informants may mirror the broader public perception of e-government services following the incidents of data breaches. However, a comprehensive assessment of public perception necessitates its own independent studies.

Trust in the capability of government agencies to deliver secure and high-quality e-services is paramount for the adoption of e-government (Liu & Carter, 2018, p. 4). This trust encompasses

both confidence in the service itself, which pertains to the safety and quality of specific e-government offerings, and trust in the government as the entity introducing these services and shaping the institutional environment in which they operate (Ibid). While the findings indicate a failure by the government to establish a sufficient institutional framework for information privacy and data protection within e-government services in The Gambia, some responsibility lies with private sector actors involved in designing these services to incorporate privacy mechanisms at the design stage. Essentially, governments heavily rely on databases, software, and devices, areas often developed and managed by the private sector (Lohmus et al., 2020). Thus, a duty exists where these private entities ought to design services whose technical aspects are compliant with data protection principles, in line with the proactive approach prescribed in the EFHR framework. Research findings, however, show that private entities contracted by the Gambian government have failed to meet this responsibility. For instance, the contracted private company, Comfort Quality Services, supplied defective QR codes on aluminium plates, compromising data security by allowing unauthorized access, thus violating the principle of restricted access. Moreover, the immigration department's data collection practices, particularly the redundant and repetitive gathering of information, contradict the principle of data minimization, questioning the efficacy of the Semlex system used for ID cards and passports. In addition, the majority of e-government services in The Gambia still rely on paper forms before data is entered into the system, potentially exposing sensitive information to risks if mishandled or improperly disposed of.

The systems designed by the private sector engineers and developers fall short of international data protection standards, particularly those advocating for data protection by design. This approach emphasizes the integration of data protection principles and practices throughout the entire data processing lifecycle, commencing from the design stage (Bygrave, 1998). This approach also confirms the proactive approach duty of engineers under the EFHR framework. However, as the private sector designs e-government services to meet the needs of the government, it is thus government’s responsibility to ensure that these services are fit for purpose and meet the recognised human rights standards for information privacy protection, and this is usually done through the creation of an enforcement mechanism. However, in the absence of an enforcement mechanism, the state can ensure compliance through the procurement process. Lohmus et al. (2020) contend that when the state acts as a discerning customer, there is a clear understanding of its needs, prompting procurement efforts to seek innovative solutions. Conversely, if the public sector fails to demand innovative solutions, it

also compels the private sector to present outdated ideas (Ibid). This thesis agrees with that premise and posits that the Gambian government can encourage and/or compel the design and implementation of e-government services that meet standards of best practice in data protection by specifying these requirements during the procurement of these e-government systems, and by stopping the use of e-government services that do not meet these information privacy and data protection standards. This way, private sector entities who develop these services are compelled to embed the appropriate data protection mechanisms in the design of these services before their implementation by government agencies. The government's capacity to mandate the development of e-government services that adhere to prescribed information privacy standards is crucial not only for addressing present breaches of data principles but also for advancing the potential for vertical integration in e-government deployment, which the research finds to be a long-term goal of the Gambian government. As vertical integration facilitates data exchange among government bodies and electronic systems through interoperability features, this necessitates enhanced security protocols to be embedded in the design of these data-sharing e-government services. Therefore, the responsibilities of the Gambian government extend beyond establishing an appropriate data protecting institutional framework for the operation of e-government services to include procuring technology that upholds human rights standards for data protection and information privacy. This is essential in ensuring that engineers of e-government services in The Gambia meet their preventive, restorative, and proactive duties under the EFHR framework. Presently, however, the Gambian government is falling short in fulfilling these obligations.

Conclusion & opportunities for further research.

There is a need for reinvention of the institutional framework under which e-government services operate in The Gambia. The knowledge created in this thesis has shown that the information privacy and data protection mechanisms currently available in e-government implementation in The Gambia fail to meet international human rights standards of best practice. The absence of a robust legal framework regulating privacy and data protection within e-government services is particularly concerning, as it contravenes both international best practices and The Gambia's own commitments under various treaties and conventions. Despite demonstrated intent, the failure to enact comprehensive legislation creates legal uncertainty and undermines accountability for privacy violations. Moreover, the lack of effective enforcement mechanisms exacerbates the situation, leaving individuals vulnerable to data breaches without recourse. Private sector involvement in designing e-government services further complicates matters, as evidenced by instances of non-compliance with human rights data protection standards. The government's reliance on private entities for technical expertise necessitates clear mandates for incorporating privacy mechanisms into service design. By specifying these requirements during procurement and halting the use of non-compliant services, the government can compel private sector actors to embed appropriate data protection measures into the design of services they develop. In essence, the Gambian government must go beyond establishing institutional frameworks to ensuring the procurement of technology conducive to upholding human rights standards for data protection and information privacy. Failure to do so not only compromises individuals' rights but also undermines public trust in e-government services, hindering the realization of their full potential for societal development and governance effectiveness.

The thesis also contributes to the theory of "engineering for human rights" by illustrating through the findings how the preventive, restorative, and proactive duties of engineers in the development of technology, can be greatly influenced by government action and/or inaction. While engineers have an important role in identifying and mitigating potential privacy risks through impact assessments as a preventive measure, the ultimate responsibility for ensuring these assessments are conducted, and for establishing a comprehensive legal framework, lies with the Gambian government. This legal framework is also essential for restorative justice for information privacy violations, and without it actions by engineer directed towards achieving this such as participating in forensic investigations to uncover violations become futile. The government can also ensure the proactive duties of engineers are met by enforcing standards

through the establishment of an enforcement/ monitoring authority, or by simply requiring that engineers meet certain standards during the procurement process.

As this thesis did not aim to assess public trust in the implemented e-government services, a potential research avenue could focus on quantitatively measuring this trust or employing a mixed-methods approach combining quantitative and qualitative methodologies. Such research could also gauge public awareness regarding their data rights and the responsibilities of data processors. Additionally, considering that a Privacy and Data Protection Bill has received cabinet approval for introduction into parliament, but has not yet been disclosed to the public, a legal examination of its provisions is warranted to assess compliance with The Gambia's obligations regarding data protection and information privacy. This analysis could also explore the practical and policy implications of the Bill's provisions.

Bibliography

Airey v. Ireland (1979) No. 6289/73, § 24, ECHR, Series A no. 32.

African Union (1981) "African Charter on Human and People's Rights" OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 http://www.oas.org/en/sla/dil/docs/African_Charter_Human_Peoples_Rights.pdf

African Union (1990) "African Charter on the Rights and Welfare of the Child" https://au.treaty-african_charter_on_rights_welfare_of_the_child.pdf

African Union (2014). "African Union convention on cyber security and personal data protection. African Union," 27. https://issafrica.org/ctafrica/uploads/AU%20Convention

Alshehri, M., Drew, S., & Alfarraj, O. (2012). "A Comprehensive Analysis of E-government services adoption in Saudi Arabia: Obstacles and Challenges." *Higher Education*, 6, pp. 8.2. https://dx.doi.org/10.14569/IJACSA.2012.030201

Alt-advisory (2023). "Africa: AU's Malabo Convention set to enter force after nine years" https://altadvisory.africa/2023/05/19/malabo-convention-set-to-enter-force/ accessed 14th Feb 2024

Ambali, A. R. (2009). "Digital Divide and its implication on Malaysian e-government: Policy initiatives." In *Social and Political Implications of Data Mining: Knowledge Management in e-Government* (pp. 267-287). https://doi.org/10.4018/978-1-60566-230-5.CH016

American Civil Liberties Union (2014) "Privacy Rights in the Digital Age: A Proposal for a New General Comment on the Right to Privacy under Article 17 of the International Covenant on Civil and Political Rights" https://www.aclu.org/sites/default/files/assets/jus14-report-iccpr-web-rel1.pdf

Anderson, P. and Dempsey, J. (2003) "Privacy and e-government: privacy impact assessments and privacy commissioners–two mechanisms for protecting privacy to promote citizen trust online." Global Internet Policy Initiative. https://www.internetpolicy.net/practices/

Belanger, F. and Hiller, J.S. (2006) "A framework for e-government: privacy implications." *Business Process Management Journal,* 12 (1), pp. 48-60. https://www.emerald.com/insight/content/doi/10.1108/14637150610643751/full/html

Benedik v. Slovenia (2018) No. 62357/14, §§ 109, 113, ECHR.

Bennett, C.J. (2000) "An international standard for privacy protection: objections to the objections. In: Proceedings of the tenth conference on Computers, freedom and privacy: challenging the assumptions" ACM, pp. 33-38. https://www.cfp2000.org/papers/bennett.pdf

Beynon-Davies, P. (2004). e-Business. New York: Palgrave Macmillan.

Bhatnagar, Subhash. 2015. "Using ICT to Improve Governance and Service Delivery to the Poor." In *Governance in Developing Asia: Public Service Delivery and Empowerment*, edited by Anil B. Deolalikar, Shikha Jha, and Pilipinas F. Quising, 296–322. Cheltenham, UK: Edward Elgar Publishing. https://doi.org/10.4337/9781784715571.

Biometric-Update, "Gambia restores Semlex contract for biometric national identity documents" Feb 16, 2018 https://www.biometricupdate.com/201802/gambia-restores-semlex-contract-for-biometric-national-identity-documents

Biometric-Update, “The Gambia launches new biometric CRVS and health insurance scheme”, Aug 8, 2022 https://www.biometricupdate.com/202208/the-gambia-launches-new-biometric-crvs-and-health-insurance-scheme

Braun V, Clarke V. (2006). “Using thematic analysis in psychology.” Quality Research in Psychology. 3(2):77–101.

Braun V, Clarke V. (2012). “Thematic analysis.” In: Cooper H, editor. APA handbook of research methods in psychology. Vol. 2, research designs. Washington (DC): American Psychological Association

Braun and Clarke, (2016) “Thematic analysis” The Journal of Positive Psychology, 2017 VOL. 12, NO. 3, 297–298 http://dx.doi.org/10.1080/17439760.2016.1262613

Buttarelli G. (2016) “Convention 108: from a European Reality to a Global Treaty.” Council of Europe International Conference, Strasbourg, 17 June. https://edps.europa.eu/sites/edp/files/publication/16-06-17_speechstrasbourg_coeen.pdf

Bygrave, L. A. (1998). “Data protection pursuant to the right to privacy in human rights treaties” Oxford University Press. International Journal of Law and Information Technology, 6(3), 247-284. https://doi.org/10.1093/ijlit/6.3.247

Cate, F.H. (1997) “Privacy in the Information Age.” Washington, D.C., Brookings Institution Press

Cavoukian, A. (2010). “Privacy by design: the definitive workshop. A foreword by Ann Cavoukian,” Ph.D. IDIS 3, 247–251 https://doi.org/10.1007/s12394-010-0062

Chacon-Hurtado, D., Kazerounian, K., Hertel, S., Mellor, J., Barry, J. J., & Ravindran, T. (2023). “Engineering for Human Rights: The Theory and Practice of a Human Rights–based Approach to Engineering.” Science, Technology, & Human Values, 1-37. https://doi-org.ezproxy.ub.gu.se/10.1177/01622439231211112

Chaffey, D. (2009). “Internet marketing: strategy, implementation, and practice.” Harlow: Financial Times Prentice Hall.

Constitute-Project (1997) “Constitution of The Gambia” https://www.constituteproject.org/constitution/Gambia_2018

Council of Europe (2018). “Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data” https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amendingthe-convention-fo/16808ac91a

Creswell, J. W. (2013). “Qualitative Inquiry & Research Design: Choosing Among Five Approaches.” Los Angeles: SAGE Publications.

Data-Guidance (2023) “The Gambia - Data Protection Overview” https://www.dataguidance.com/notes/gambia-data-protection-overview

Davies, S. (1996). “Big Brother: Britain's web of surveillance and the new technological order.” Pan, London.

De Aguiar Borges, G. O. (2023). “Navigating Human Rights in the Digital Age: An Exploration of Data Protection Laws in Brazil and in Europe.” Beijing law Review, 14, 1772-1789. https://doi.org/10.4236/blr.2023.144098

ECOWAS, (2010) “Supplementary Act on Personal Data Protection within ECOWAS” A/SA.1/01/10 https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf

Eisenhardt, Kathleen. M. and Graebner, Melissa. E. (2007) Theory building from cases: Opportunities and challenges. Academy of management journal, 50(1), 25-32. https://psycnet.apa.org/doi/10.5465/AMJ.2007.24160888

European Union, (2016). “General Data Protection Regulation” Regulation (EU) 2016/679 https://gdpr-info.eu/

Global Internet Liberty Campaign. (n.d.). “Privacy and Human Rights: An International Survey of Privacy Laws and Practice.” Retrieved from https://gilc.org/privacy/survey/intro.html#fnlnk0009 on the 14th of Feb. 2023.

Global-Voices, (2022) “The Gambia launches digital immunization registry” https://globalvoices.org/2022/07/06/the-gambia-launches-digital-immunization-registry/ ,original version first published on The Alkamba Times at, June 21, 2022 “The Gambia Becomes the First country in Africa to Introduce a Digital Immunization Registry” https://alkambatimes.com/the-gambia-becomes-the-first-country-in-africa-to-introduce-a-digital-immunization-registry/ accessed 13 Feb 2023

GMCSIRT, (2019) “Data Protection and Privacy Policy” https://gmcsirt.gm/wp-content/uploads/2021/12/Data-Protection-and-Privacy-Policy-and-Strategy-August-2019-Final.pdf

Greenleaf G. (2018) “The UN should adopt Data Protection Convention 108 as a global treaty: Submission on 'the right to privacy in the digital age' to the UN High Commission for Human Rights, to the Human Rights Council, and to the Special Rapporteur on the Right to Privacy.” Sydney, 8 April 2018. https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/GrahamGreenleafAMProfessorLawUNSWAustralia.pdf

Grunden, K. (2012) “A Social Perspective on the Implementation of e-Government: A Longitudinal Study at the County Administration of Sweden.” *Case Studies in E-Government,* 1, pp. 120. https://www.semanticscholar.org/paper/A-Social-Perspective-on-Implementation

Hanno N Olinger, Johannes J Britz and Martin S Olivier, (2007) “Western Privacy and/or Ubuntu? Some Critical Comments on the Influences in the Forthcoming Data Privacy Bill in South Africa” 39 The International Information & Library Review 31, 34.

Harb, Y. and Abu-Shanab, E. (2009) “The impact of e-government on rural areas: the case of Jordan”, Third Mosharaka International Conference on Communications, Computers and Applications, pp.1–6, Amman, Jordan.

HealthCare Africa, (2022) “Gambia institutes digital birth certificates, National Health Insurance” https://www.healthcareafrica.info/gambia-institutes-digital-birth-certificates-national-health-insurance/

Heeks, R. (2001). “Building e-governance for development: A framework for national and donor action.” University of Manchester. Institute for Development Policy and Management. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3540057

Hixson, R. (1987). “Privacy in a Public Society: Human Rights in Conflict.” Oxford University Press.

Hook, C, (1989) “Data Protection Implications for Systems Design.” NCC Publications, Manchester

International Covenant on Civil and Political Rights. (19 December 1966). 999 UNTS 171, Can TS 1976 No 47 (entered into force 23 March 1976) [ICCPR].

J. A. Shamsi and M. A. Khojaye, (2018) "Understanding Privacy Violations in Big Data Systems," in IT Professional, vol. 20, no. 3, pp. 73-81

Kelly, S. (2010). "Qualitative interviewing techniques and styles." In: Bourgeault, I., Dingwall, R., & de Vries, R. (eds), The Sage Handbook of Qualitative Methods in Health Research. Thousand Oaks: Sage Publications. https://www.semanticscholar.org/paper/Qualitative-Interviewing-Techniques-and-Styles-Kelly/

Kitchin, R. (2014). "Big Data, New Epistemologies and Paradigm Shifts. Big Data & Society", 1(1), 1-12. https://doi.org/10.1177/2053951714528481

Law-hub Gambia (2024) "History of Constitutional Making in The Gambia" https://www.lawhubgambia.com/constitution-making-history.

Women's Act (2010) https://www.lawhubgambia.com/womens-act-2010.

Legal Resources Centre. (2018) "Recommended Resolution to the NGO Forum" https://privacyinternational.org/sites/default/files/2018.pdf

Liu, D. & Carter, L. (2018) "Impact of Citizens' Privacy Concerns on e-Government Adoption" https://dl-acm-org.ezproxy.ub.gu.se/doi/pdf/10.1145/3209281.3209340

Lohmus, K., Nyman-Metcalf, K., Ahmed, R.K., Pappel, I., and Draheim, D. (2020) "The Private Sector's Role in e-Government from a Legal Perspective" , Fourth International Congress on Information and Communication Technology, Advances in Intelligent Systems and Computing 1027, https://doi.org/10.1007/978-981-32-9343-4_22

Marshall MN. (1996) "The key informant techniques. Family Practice" Oxford University Press; 13: pp. 92-97. 13-1-92.pdf (silverchair.com)

Meena, J. and Sagar, N. (2010) "E-governance & good governance", International Referred Research Journal, October, ISSN-0974-2832, Vol. 2, No. 21, pp.8–10.

Michael, J. (1994). "Privacy and human rights: An international and comparative study, with special reference to developments in information technology." Paris, France: UNESCO; Aldershot, Hampshire, England: Dartmouth Pub. Co. https://archive.org/details/privacyhumanrigh0000mich

Miller, H. (2013). From 'rights-based' to 'rights-framed' approaches: a social constructionist view of human rights practice. Journal of Human Rights Practice, 5(2), 288-309. https://doi.org/10.1080/13642987.2010.512136

Moore, B. (1984). "Privacy: Studies in Social and Cultural History." Armonk, N.Y.: M.E. Sharpe; Distributed by Pantheon Books.

Munyoka, W. & Maharaj, M.S. (2019) "Privacy, security, trust, risk and optimism bias in e-government use: The case of two Southern African Development Community countries", South African Journal of Information Management 21(1), a983. https://doi.org/10.4102/

Mutimukwe C, Kolkowska E, Grönlund Å. (2019) "Information privacy practices in e-government in an African least developing country, Rwanda." p. 1-21, E J Info Sys Dev Countries.; 85: e12074. https://doi.org/10.1002/

"Data Protection Act" (2012) https://nita.gov.gh/theevooc/2017/12/Data-Protection-Act-2012-Act-843.pdf

Ndou, V. (2004). "E-government for developing countries: opportunities and challenges." The Electronic Journal of Information Systems in Developing Countries, 18. https://onlinelibrary.wiley.com/doi/10.1002/j.1681-4835.2004.tb00117.x

Nkonko M Kamwangamalu, (1999) "Ubuntu in South Africa: A Sociolinguistic Perspective to a Pan-African Concept" 13 Critical Arts 24, 27.

OCCRP, (2020) "Biometric Bribery: Inside Semlex's Global Playbook", , https://www.biometricupdate.com/201802/gambia-restores-semlex-contract-for-biometric-national-identity-documents

Okeyo, N. O. (2022) "Data Protection Impact Assessment as a Human Rights Duty of State" Afronomics Law pp. 1-7 https://www.afronomicslaw.org/print/pdf/node/2491

Otley, D. T., & Berry, A. J. (1994). "Case study research in management accounting and control. Management Accounting Research" 5(1), 45-65. Kidlington: Elsevier Ltd.

Orji, Uchenna J. (2017) "Regionalizing data protection law: a discourse on the status and implementation of the ECOWAS Data Protection Act" International Data Privacy Law, 2017, Vol. 7, No. 3, pp. 179-189 https://academic.oup.com/idpl/article-abstract/7/3/179/4211051?redirectedFrom=fulltext

Peck v. the United Kingdom (2003) No. 44647/98, § 57, ECHR 2003-I.

Pidgeon, N. F., Turner, B. A., & Blockley, D. I. (1991). "The use of Grounded Theory for conceptual analysis in knowledge elicitation." International Journal of Man-Machine Studies, 35(2), 151-173. https://doi.org/10.1016/S0020-7373(05)80146-4

Pina, V., Torres, L., & Royo, S. (2009). "E-government evolution in EU local governments: A comparative perspective. Online Information Review," 33(6), 1137-1168. https://doi.org/10.1108/14684520911011052

Pisa, M., Nwankwo, U., & Dixon P. (2021) "Why Data Protection Matters for Development: The Case for Strengthening Inclusion and Regulatory Capacity" https://www.cgdev.org/publication/why-data-protection-matters-development-case-strengthening-inclusion-and

Pleger, L. E., Guirguis, K., & Mertes, A. (2021) "Making public concerns tangible: An empirical study of German and UK citizens' perception of data protection and data security" Computers in Human Behavior, Vol. 122, pp. 1-17 https://www.sciencedirect.com/science/article/pii/S0747563221001539

Popiel, P. & Schwartz-Henderson, L. (2022) "Understanding the Challenges Data Protection Regulators Face: A Global Struggle Towards Implementation, Independence, & Enforcement". Adapt https://adapt.internews.org/wp-content/uploads/2022/07/DataProtectionRegulators_July2022_ADAPT.pdf

Reuters (2018). "In Africa, scant data protection leaves internet users exposed". Written by Maggie Fick and Alexis Akwagyiram https://www.reuters.com/article/idUSKCN1HB1UE/

Children's Act (2005). https://www.studocu.com/row/document/university-of-the-gambia/criminal-law-ii/childrens-act-2005-theres-no-description/42041492

Rogers Everett, M., (2003). "Diffusion of innovations." (5th ed.). New York: Macmillan Publishing.

Singh, A., & Power, M. (2019). "The privacy awakening: the urgent need to harmonise the right to privacy in Africa." African Human Rights Yearbook, 3, 202-220. http://doi.org/10.29053/2523-1367/2019/v3a10

State Assembly (2023) "State of The Nation Address" https://www.assembly.gm/wp-content/uploads/STATE-OF-THE-NATION-ADDRESS-2023-PRESIDENT.pdf

Strauss, A. L., & Corbin, J. (1998). "Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory" (2nd ed.). Thousand Oaks, CA: Sage.

Takahashi, A. R. W., & Araujo, L. (2019). "Case study research: Opening up research opportunities." RAUSP Management Journal, ISSN: 2531-0488. https://www.emerald.com/content/doi/10.1108/

The Standard Newspaper (2020). "Comfort Quality Services supplies Police with 100 QR scanners" https://standard.gm/comfort-quality-services-supplies-police-with-100-qr-scanners/

Tyrer v. the United Kingdom (1978) No. 5856/72, § 31, ECHR, Series A no. 26.

UNESCO. (2005). "E-government toolkit for developing countries." Available at: http://unesdoc.unesco.org/images/0013/001394/139418e.pdf [Accessed 6th Feb. 2024]

UN General Assembly. (1948). "Universal declaration of human rights" (217 [III] A). Paris.

UN Human Rights Committee, "General Comment 16." (Issued 23 March 1988). UN Doc A/43/40, 181–183; https://www.refworld.org/legal/general/hrc/1988/en/27539

UN Human Rights Committee "General comment 34" (Issued 12 September 2011). CCPR/C/GC/34 https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf

UN Human Rights Council (2013) "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" paragraph 15 https://digitallibrary.un.org/record/756267?ln=en&v=pdf

UN Human Rights Council (2024) "Legal safeguards for personal data protection and privacy in the digital age: Report of the Special Rapporteur on the right to privacy, Ana Brian Nougrères A/HRC/55/46 https://www.ohchr.org/en/documents/thematic-reports/ahrc5546-legal-safeguards-personal-data-protection-and-privacy-digital

UN Human Rights Treaty Bodies (2024) "UN Treaty Body Database" https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?Treaty=CCPR

Uzun v. Germany (2010) No. 35623/05, §§51-52, ECHR

Wescott, C. (2003). "E-government to combat corruption in the Asia Pacific Region." In: Prepared for the 11th International Anti-Corruption Conference. Seoul, Republic of Korea. https://ieeexplore.ieee.org/abstract/document/4680403

Westin, A.F. (1967) "Privacy and freedom". (1st ed.) Atheneum, New York

Wu, Yuehua (2014) "Protecting personal data in E-government: A cross-country study" Government Information Quarterly, Vol. 31, Issue 1, pp. 150-159 https://doi.org/10.1016/j.giq.2013.07.003

Yohannes Eneyew Ayalew (2023). "The African Union's Malabo Convention on Cyber Security and Personal Data Protection enters into force nearly after a decade. What does it mean for Data Privacy in Africa or beyond?". European Journal of International Law, vol. 34, no. 3 https://www.ejiltalk.org/malabo-convention-on-cyber-security-and-personal-data-protection

Yin, Robert. K. (2009). “Case Study Research: Design and Methods”. Los Angeles, CA: Sage Publications.

Z. v. Finland (1997) No. 22009/93, §§ 95-96, ECHR, Reports of Judgments and Decisions 1997-I

Annexes.

Annex 1

Interview Guide	
Question	**Purpose of the question**
1. Please describe your involvement in the digital technology space in The Gambia?	To provide information on the expertise of the informant
2. What in your opinion is the goal of implementing e-governance systems in The Gambia?	To gauge Informants' understanding of the motivations and objectives behind the implementation of e-governance systems in The Gambia. Responses can provide insight into the socio-political context of The Gambia, as well as the potential benefits and challenges associated with e-governance initiatives.
3. How is data collected, processed and stored through these services?	To solicit detailed information on the realities of e-government service delivery in The Gambia particularly in the context of data processing.
4. To what extent are privacy and data protection mechanisms incorporated into these e-government service(s)?	To establish in detail what current privacy and data mechanisms currently exist in the context of e-government implementation in The Gambia. Also to evaluate the effectiveness of existing mechanisms for safeguarding user data within e-government systems, as well as potential areas for improvement in data security practices.
5. What are your own personal recommendations to improve these systems in light of privacy and data protection standards?	By providing recommendations, informants are also able to identify the most pressing issues related to privacy in e-government systems and potentially suggest appropriate solutions to them.
6. Is there anything you would like to raise that we have not talked about?	To provide interviewees with an opportunity to discuss other factors associated with privacy and data protection in e-Government implementation in The Gambia.

Annex 2

Are you interested in taking part in the research project?
Privacy and data protection in e-government services in The Gambia: A human rights perspective

Purpose of the project You are invited to participate in a research project. The main purpose is to describe to what extent are privacy and data protection mechanisms incorporated into the delivery of e-government services in The Gambia. The rapid digitalization of government services in The Gambia necessitates the extensive collection, storage, and processing of personal data of private individuals on a large scale. However, the process and its execution are currently opaque, with no existing literature providing detailed information. Questions pertaining to the collection, processing, storage of data, and the rights of those who provide the data remain unanswered in the literature. This thesis aims to unravel this entire process, particularly seeking to explore the extent to which data collecting systems within public services in The Gambia incorporate privacy and data protection mechanisms that align with human rights standards.

Which institution is responsible for the research project?
University of Tromso is responsible for the project (data controller).

Why are you being asked to participate?
Firstly, the thesis will use the doctrinal approach to examine documents detailing the existing legal and regulatory framework with regards privacy and data protection in The Gambia. This would establish what the law says about privacy and data protection in The Gambia and would provide a basis of comparison to what happens in the actual daily practice of data collection, processing and storage in The Gambia to see if the practice reflects the regulations. To ascertain what happens in practice, insights from stakeholders (such as yourself) in the data protection space in The Gambia would be collected through a number of semi-structured interviews. Due to your expertise on this topic, the expectation is that key informants provide valuable insights into the challenges and opportunities associated with these data collecting national digital systems.

What does participation involve for you?
If you choose to take part in the project, this will involve a semi-structured interview that will take approx. 30 minutes. The interview includes questions about how data is collected, processed and stored in The Gambia; parties responsible; and whether privacy and data protection mechanisms have been incorporated into these e-government systems. Your answers will be recorded electronically.

Participation is voluntary Participation in the project is voluntary. If you chose to participate, you can withdraw your consent at any time without giving a reason. All information about you will then be made anonymous. There will be no negative consequences for you if you chose not to participate or later decide to withdraw.

Your personal privacy – how we will store and use your personal data
We will only use your personal data for the purpose(s) specified here and we will process your personal data in accordance with data protection legislation (the GDPR). Only the researcher will

have access to the data collected. I will implement strict access controls and authentication mechanisms. This includes strong password policies, multi-factor authentication, and limiting access to the devices storing this data. I will also encrypt the data collected, both in transit and at rest. This ensures that even if unauthorized access occurs, the data remains unreadable without the proper decryption keys.
Each participant would grant consent regarding to what extent they want to be recognizable in the publication. These identifiers may include name, occupation, and relevant expertise or involvement in the data protection space in The Gambia.

What will happen to your personal data at the end of the research project?
The planned end date of the project is 23rd of May, 2023. The collected data will be anonymised at the end of the project.

Your rights

- So long as you can be identified in the collected data, you have the right to:
- access the personal data that is being processed about you
- request that your personal data is deleted
- request that incorrect personal data about you is corrected/rectified
- receive a copy of your personal data (data portability), and
- send a complaint to the Norwegian Data Protection Authority regarding the processing of your personal data

What gives us the right to process your personal data?
We will process your personal data based on your consent.
Based on an agreement with the University of Tromso, The Data Protection Services of Sikt – Norwegian Agency for Shared Services in Education and Research has assessed that the processing of personal data in this project meets requirements in data protection legislation.
Where can I find out more?
If you have questions about the project, or want to exercise your rights, contact:

- UiT Arctic University of Norway via Nasiru Deen (email: nasirudeen3883491@gmail.com)
- UiT Arctic University of Norway via Jennifer Hays (email: Jennifer.hays@uit.no)
- Our Data Protection Officer: Anniken Steinbakk (email: personvernombud@uit.no)

If you have questions about how data protection has been assessed in this project by Sikt, contact:

- email: (personverntjenester@sikt.no) or by telephone: +47 73 98 40 40.

Yours sincerely,
Project Leader Student (if applicable)
(Researcher/supervisor)

Consent form

I have received and understood information about the project '*Privacy and data protection in e-government services in The Gambia: A human rights perspective'* and have been given the opportunity to ask questions. I give consent:

- to participate in a 30-minute semi-structured interview
- for information about me to be published in a way that I can be recognised (describe in more detail)– if applicable

I give consent for my personal data to be processed until the end of the project.

(Signed by participant, date)