<http://www.diva-portal.org>

Postprint

This is the accepted version of a paper published in *Electronic Journal of Information Systems in Developing Countries*. This paper has been peer-reviewed but does not include the final publisher proof-corrections or journal pagination.

Citation for the original published paper (version of record):

Mutimukwe, C., Kolkowska, E., Grönlund, Å. (2019)
Information privacy practices in eGovernment in an African Least Developing Country, Rwanda
Electronic Journal of Information Systems in Developing Countries, 85(2): e12074
<https://doi.org/10.1002/isd2.12074>

Access to the published version may require subscription.

N.B. When citing this work, cite the original published paper.

Permanent link to this version:

<http://urn.kb.se/resolve?urn=urn:nbn:se:oru:diva-71433>

Information privacy practices in eGovernment in an African Least Developing Country, Rwanda

In press, Electronic Journal of Information Systems in Developing Countries, December 2018

Chantal Mutimukwe^{1,2} | **Ella Kolkowska**¹ | **Åke Grönlund**¹ |

¹Department of Informatics, School of Business, Örebro University, Sweden

² Department of Computer and Software Engineering, School of ICT, College of Science and Technology, University of Rwanda

Correspondence:

Chantal Mutimukwe, Department of informatics, School of Business, Örebro University, Sweden

Email: Chantal.mutimukwe@oru.se

Abstract

Privacy of information is a critical issue for e-government development as lack of it negatively influences users' trust and adoption of e-government. To earn user trust government organizations need to provide reliable privacy assurance by implementing adequate information privacy protection (IPP) practices. African Least Developing Countries (LDCs) today develop e-government but focus is on quick technical development and the status of IPP issues is not clear. Little research has yet studied the status of IPP practices in e-government in African LDCs. To fill this gap, we assess the status of existing IPP practices in e-government in Rwanda, using international privacy principles as an assessment baseline. We adopt a case-study approach including three cases. Data were collected by interviews and a survey. The findings call into question the efficacy of existing IPP practices and their effect in ensuring e-government service users' privacy protection in Rwanda. The study extends existing literature by providing insights related to privacy protection from an African LDC context. For practitioners in Rwanda and other

LDCs, this study contributes to the protection of information privacy in e-government by providing recommendations to mitigate identified gaps.

Keywords: Information privacy practices, privacy principles, e-government, African LDCs, Rwanda.

1. Introduction

E-government is defined as the use of information technology (IT), especially the Internet, to deliver government services and information to citizens, businesses, and other government bodies (Holden, Norris, & Fletcher, 2003). One of the benefits of internet use for service delivery is the possibility to easily collect, store, process and disseminate citizens' personal information (Libaque-Sáenz, Wong, Chang, Ha, & Park, 2016) accurately and in real time. Personal information is information making specific individuals identifiable (AICPA & CICA, 2011 pp.1). Government organizations rely on such information to increase the efficiency and effectiveness of government decision making (Kim, Trimi, & Chung, 2014; Welch, Feeney, & Park, 2016), enhance transparency, accountability in service delivery and empower innovation (Chen & Hsieh, 2014).

Although government organizations gain benefits from extended collection, storage and dissemination of personal information, these activities often rise users' concerns for possible violations of their privacy (McDonagh, 2002; Smith, Milberg, & Burke, 1996; Solove, 2006). As information technology advances, e-government users' privacy concerns are getting bigger as more data is collected and used for various purposes including more in-depth analyses and to make services more efficient (CIGI & Ipsos, 2018).

The literature shows that ensuring privacy of citizens information and addressing their privacy concerns is crucial for adoption of e-government as it influences users' trust and willingness to use e-government services. (Abu-Shanab, 2014; Akkaya, Wolf, & Krcmar, 2012; Belanger & Carter, 2008; Verkijika & De Wet, 2018). To fully unleash the potential and benefits of e-government, government organizations need to adopt IPP (information privacy protection) practices to ensure citizens that their personal information is protected.

In developed countries IPP practices are reflected in national and international regulations (Wright & Raab, 2014) and commonly used to protect users' privacy (Chua, Herbland, Wong & Chang, 2017 pp. 159). In African Least Developed Countries (LDCs) development of IPP practices is lagging behind (Borena, Bélanger, & Ejigu, 2015; Makulilo, 2015; Yilma, 2017), which is a serious problem since, like everywhere else, information privacy (IP) is a challenge to citizens' trust and acceptance of e-government in those countries (Nkwe, 2012). Despite this, researchers in information systems have so far scarcely addressed the issue of privacy protection

in e-services in an African context (Bélanger & Crossler, 2011; Makulilo, 2012; Nwaeze, Zavorsky, & Ruhl, 2017).

The present study contributes to the literature by reporting on existing IPP practices in e-government in Rwanda, an LDC in Eastern Africa with high ambitions for not just e-government but generally for IT and moving into the information society, and with a good development record for the past two decades (Mwangi, 2006; UNPAN, 2016). Mutimukwe, Kolkowska & Grönlund (2017) show that citizens in Rwanda are concerned about their privacy when interacting with e-government services and some even refuse to provide personal information. Privacy protection is considered to be one of the most important issues to take care of in an ambition to transform the country into a digital hub for the Continent of Africa (Nsengimana, 2017). Following prior studies (Al-Jamal & Abu-Shanab, 2015; Marotta-Wurgler, 2016; Nwaeze et al., 2017; Stanaland & Lwin, 2013) we use international principles as an assessment tool. Our study differs from previous studies (Nwaeze et al., 2017; Verkijika & De Wet, 2018) assessing IPP practices in e-government in Africa since we focus on actions inside the organizations (e-government service providers). Therefore our study, besides adding to general knowledge of privacy protection in e-government in Africa also contributes to increased understanding of how privacy practices are carried out within e-government organizations in an African LDC context. By highlighting the problems in existing IPP practices we also expect to contribute to the development of robust IPP practices in e-government in Rwanda.

The rest of the paper is organized as follows: Section 2 gives an overview of IPP practices and the status of those practices in African LDCs. It is followed by section 3 which discusses different international privacy principles taken as theoretical lens for this study. Then, section 4 briefly presents the research settings, and it mainly describes the selected cases studies. In section 5, the methods used for data collection and analysis are presented. Section 6 presents the research findings, followed by section 7 which discusses these findings along with their implications. Section 8 concludes the paper.

2. Information privacy practices and African LDCs context

IPP practices are activities taken to protect users' information privacy while using e-services (Culnan & Bies, 2003; Murphy, Reddy, & Xu, 2014; Stanaland & Lwin, 2013). IPP practices include government regulation, organizational self-regulation, and technological solutions (Borena et al., 2015; Culnan & Bies, 2003). Government organizations need to adopt IPP practices that deal with all kinds of privacy issues pertaining to e-government activities.

2.1 Government regulations

Governments are required to enact laws, inspect their implementation, and monitor changes in processes and activities by different actors who can violate citizens' IP (Borena et al., 2015; Xu, Teo, Tan, & Agarwal, 2012). The basic intention of these laws is to facilitate lawful use of information while protecting IP at the national level.

In developed countries, governmental privacy regulations is established and used for a long time – while still evolving – but such regulation is largely lacking in the African LDCs (Borena et al., 2015). Yilma (2017) showed that in 2015 none of the East African countries (Rwanda, Burundi, Tanzania, Uganda, and Kenya) had specific privacy regulations to guide the implementation of privacy practices. Although these countries mention privacy in their constitution and/or common laws, the regulation is not sufficient for protecting IP in e-services (Makulilo, 2015).

Nwaeze, Zavarsky, & Ruhl (2017) showed that out of five West Anglophone African countries only Ghana has a privacy protection regulation. Nwaeze, Zavarsky, & Ruhl (2017) evaluated the content of privacy protection regulations of the Anglophone West African countries (Ghana, Nigeria, Sierra Leone, Liberia, and Gambia) using the ISO/IEC 29100:2011 privacy principles as a baseline for the evaluation. They found that Ghana was the only country out of the five studied which had a sufficient data and privacy protection regulation, but despite the existence of that regulation, most of the evaluated e-government websites in Ghana did not comply with the regulation

Verkijika and de Wet (2018), evaluated 279 e-government websites from 31 countries in Sub-Saharan Africa, based on a public value perspective, including privacy and security of citizens' information. They found that only 14% of the evaluated e-government websites had a privacy

policy and that most of the websites did not have any visible privacy statements. They also found that security at the studied websites was very low, which put users' personal information at risk.

2.2 Self-regulation

Self-regulation means that organizations develop policies and enforcement strategies that supplement government regulations (Xu, Dinev, Smith, & Hart, 2011). While government regulations are general and apply to all kinds of organization, self-regulation is specific to the organization (Xu, Bagby, & Melonas, 2009).

Effective self-regulation requires organizations to adopt and implement privacy policies that are based on governmental regulations and international privacy principles. Implementing privacy policies requires effective compliance procedures and enforcement mechanisms so users can trust that the organization is acting by the rules and that there will be sanctions in case it does not (Culnan & Bies, 2003). Sometimes, self-regulation practices involve a contractual relationship between an organization and an assurator (third party) whose duty it is to measure the extent to which the organization complies with its privacy policies (Xu et al., 2011, 2012). The assurator provides a privacy seal to inform users that their IP is protected as stated by the principles defining the seal. One example of a privacy seal is TRUSTArc (formerly TRUSTe). According to previous studies, e.g. Borena et al. (2015), privacy self-regulation in African LDCs is almost non-existing.

2.3 Technological solutions

Privacy Enhancing Technologies (PETs) are generally any technology that is designed to protect or promote the privacy interests of individuals (Xu, Bagby, & Melonas, 2009). PETs usually put more emphasis on the confidentiality aspect of security, more specifically on hiding the identities of individuals or their personal data (Heurix, Zimmermann, Neubauer, & Fenz, 2015). Organizations configure PETs according to pertinent self-regulations and/or government regulations (Argyakis, Gritzalis, & Kioulafas, 2003). There exist numerous types of PETs. (Heurix, Zimmermann, Neubauer, & Fenz, 2015). Pelkola (2012) classified them into six categories: system security access controls, data encryption, authorization based on defined user

profiles, biometric authentication, data separation, and data anonymization. Borena et al. (2015) argued that use of PETs does not seem viable in Africa due to limited resources and lack of knowledge and skills to implement and use them.

This brief review shows that both government regulation and self-regulation are not well developed in African countries. While we do not know the extent to which PETs are used, clearly they are mainly focused on security and while a potentially powerful tool for that purpose they cannot remedy all privacy issues.

3. Information privacy principles

Information privacy principles concern conditions and/or guidelines for developing information privacy practices (Al-Jamal & Abu-Shanab, 2015), and have been identified as an essential baseline for assessing such practices (Wright & Raab, 2014). There exist numerous sets of such principles with different scope. We reviewed several previous studies assessing IP practices in different countries and regions (Al-Jamal & Abu-Shanab, 2015; Dayarathna, 2013; Marotta-Wurgler, 2016; Maumbe, Owei, & Alexander, 2008; Nwaeze et al., 2017; Oetzel & Spiekermann, 2014; Stanaland & Lwin, 2013; Stewart, Kane, & Storey, 2006; Wright & Raab, 2014; Wu, Huang, Yen, & Popova, 2012) and found that the most commonly used sets of principles are : 1) The OECD (Organization for Economic Co-operation and Development) principles 2) the Fair Information Practice (FIP), 3) International standard for privacy principles developed by International Standards Organization (ISO), 4) the General Accepted Privacy (GAP) principles by the Canadian Institute of Chartered Accountants and the American Institute of Certified Public Accountants, and 5) the European General Data Protection Regulation (GDPR).

These five sets of principles are widely recognized. While none of them is more accepted than others (Dayarathna, 2013), globalization has increased the importance of shared principles and led to the most recent one, GDPR, affecting most organizations in the world as it sets mandatory principles for not only the EU but for every organization doing any business with the EU. Each set is applied and considered as important in a certain context or region. However, the different sets of IP principles are more or less comprehensive, have considerable overlaps and sometimes use different terms referring similar issues (Al-Jamal & Abu-Shanab, 2015). Dayarathna (2013)

argued that this inconsistency brings difficulties in understanding and using the principles for privacy risk classification and assessment.

To cover all important aspects but avoid redundancy of issues, Al-Jamal & Abu-Shanab, (2015) matched OECD (the Organization for Economic Cooperation and Development) and FTC (The Federal Trade Commission) sets of principles into a new, more comprehensive set. By comparing definitions of the principles included in OECD and FTC, the authors found, that one principle of FTC could correspond to two principles of OECD. For instance, *notice* of FTC corresponds to *collection limitation* and *purpose specification* of OECD. The authors also found that *data quality* principle of OECD didn't match with any principle of FTC principles. As in our evaluation of IPP practices in Rwanda we wanted to cover as many aspects as possible, we chose to merge the five most commonly used sets of IP principles into a one comprehensive set.

Following Al-Jamal & Abu-Shanab, (2015), we merged the sets by comparing the definitions of each principle included in the five sets of principles: OECD (includes 8 principles), FIP (5 principles), ISO (11 principles), GAP (10 principles), GDPR (7 principles). Definitions of all these principles are provided in Appendix 1. We categorize the principles by gathering common elements into a single category, as illustrated in table 1. In some cases, elements of one principle could be included in more than one category. For example, elements of, *openness, transparency, and notice* (ISO) were categorized into *notice and awareness* as well as *accountability*. Each category was then labeled and defined based on the included elements. For instance, the category *notice and awareness* includes all elements concerning notifying users (data subject) about activities related to the collection, use, or extended use of their information, together with an explanation why the information is used. *Notice and awareness* includes elements of *principles notice and collection* of GAP, *purpose specification, individual participation and openness* of OECD, *openness, transparency, and notice* of ISO, and, *notice and awareness* of FIP (see table 1). In this way we formulated a new set of seven principles presented in Table 1.

4. Research setting

4.1 eGovernment and information privacy in Rwanda

This research is based on case studies conducted in Rwanda. Rwanda is a small (26,388 km²) and landlocked country located in East Africa, with an estimated population of some 11.9 million and

a per capita GDP of 703 USD (World Bank, 2016). The Rwandan economy is based largely on agricultural production with 88% of the population engaged in (mainly subsistence) agriculture.

Striving to reduce poverty, the Government of Rwanda formulated the Vision 2020 policy, the over-arching aim of which is to transform the country into a knowledge-based, middle-income society and modernize agriculture (Rwanda, 2012). The Government of Rwanda identified advancing science, technology, and information and communication technology (ICT) as an approach to achieving this vision. It considers ICT a central engine to the knowledge-based economic development and a tool that can enable Rwanda to leap-frog the key stages of industrialization. In that line, since 2005, the government of Rwanda has initiated e-government projects intended mainly to facilitate government service delivery to citizens and businesses and bring people closer to the government using ICT. So far, notable progress has been achieved, and e-government is changing the service-delivery scheme. The most recent UN e-government survey ranked Rwanda among top 10 African countries (out of 54) with a high e-government development index (0.4590) (UNDESA, 2018). Initiatives that have been implemented include the “IREMBO,” a portal to e-government services, as well as different tax declaration and payment utilities and many other online service applications.

The interaction between citizens and e-government services also requires a legal infrastructure to address, among other things information privacy protection. Although Rwanda has not yet passed a national privacy regulation, there are other initiatives to harmonize IP protection. For instance, articles 124, 209, and 213 of the recently established law governing ICT focus on privacy protection in collection and processing of personal information (The Republic of Rwanda, 2016). Article 23 of the Rwanda Constitution mentions the protection of, and respect for, the right to privacy (The Republic of Rwanda, 2015). Other laws that are related to individuals’ right to privacy are in place include No. 02/2013 regulating media (article 9), No. 03/2013 regulating access to information (article 4), and No. 60/2013 regulating the interception of communication (Human Rights Committee, 2015).

4.2 Description of the cases

We selected three cases: RwandaOnline, Rwanda Revenue Authority, and Rwanda Land Management and Use Agency to assess IPP practices in an e-government context in Rwanda.

RwandaOnline: In its quest to speed up and synchronize e-government implementation, the Government of Rwanda entered into a public-private partnership with the private company RwandaOnline Ltd (ROL). ROL is assigned to build, operate, and transfer (BOT) a single window national platform (portal) called IREMBO for the delivery of government services over the Internet. According to the agreement, ROL is contracted to build and operate the IREMBO platform for 25 years. In a first step 100 e-services were planned to be available by the end of 2017. A visit on IREMBO (The Republic of Rwanda, n.d.) on September 28, 2017, showed that it hosted 95 online services including birth, marriage, and death certificates, land management services (registration, transfer, merging, subdivision, and building permits), transportation licenses, insurance licenses, criminal records, and motor vehicle inspection. In most cases using e-services is mandatory since the corresponding manual procedures are not used any more. Rwandans can access IREMBO services via computers or phones or visit an IREMBO service office or an IREMBO agent for assistance. IREMBO agents are private businesses that assign agreement with ROL to assist citizens throughout the services application processes.

To operate IREMBO, ROL involves stakeholders from private companies such as banks and telecommunication companies in the partnership. It also involves local public offices who are the providers of the majority of services that are made available on the IREMBO platform. Other stakeholders are the Ministry of ICT and Innovation, Rwanda Information Society Authority, and the Rwanda Governance Board who all are in charge of implementation and monitoring of IT projects in Rwanda. For government organizations, IREMBO provides an interface for receiving applications and communicating with citizens and businesses regarding the status of their applications. The back-office operations are managed by, and the responsibility of, corresponding government agencies. ROL was chosen as the first case study as it manages the common e-government portal, while at the same time being a large e-government project, with different government organizations being involved.

Rwanda Land Management and Use Authority (RLMUA): One of the agencies that operate as back office for IREMBO services is the Rwanda Land Management and Use Authority (RLMUA). RLMUA's overall objective is to put in place an efficient system of land administration and land management that secures land ownership, promotes investment in land for socio-economic development, and contributes to poverty reduction (RLMUA, 2017). RLMUA

introduced the Land Administration Information System (LAIS), a web based land registration tool developed in order to ensure a proper land management and land administration, specifically the maintenance of land certificates issued to landholders during land registration (Ministry of Natural Resource, 2012). LAIS is expected to help reducing transaction time and costs, as well as improving the reliability of the land registry and reducing land disputes. Some of services within LAIS, such as land transfers, land registration and land sub-division, are accessed through IREMBO, and LAIS is one of the biggest repositories of services at IREMBO. The front end of LAIS is operated by ROL while RLMUA plays the role of the back office. RLMUA was added as a second case study because it illustrates the integration between the front-end and back-end of the services.

Rwanda Revenue Authority (RRA): Although IREMBO is supposed to be a comprehensive e-government portal, there are many e-government services that cannot, so far, be accessed through it. Those include all services related to tax payment and declaration, which are managed by the Rwanda Revenue Authority (RRA). RRA is the single government revenue collection agency in Rwanda. RRA has been charged to take advantage of the numerous opportunities afforded by information and communication technologies to facilitate tax collection, reduce corruption, and save time and money in the tax payment process. RRA has thus far introduced three online applications including e-filing, Rwanda Electronic Single Window, and e-payment (also called e-tax). E-filing offers clients the opportunity to file taxes such as the value-added (VAT), pay-as-you-earn (PAYE), excise duty, and withholding taxes electronically on the RRA website without having to visit RRA offices. E-filing is complemented by an e-payment system that enables a taxpayer, after declaring taxes online, to also pay online. The Rwanda electronic Single Window (ReSW) is an online customs clearing utility. The system allows traders to register information with a single web-based portal to fulfill all import- and export-related regulatory requirements. RRA was selected for this study so as to reflect other government services that are accessible outside of the national portal (IREMBO). Similar to IREMBO, Rwandans can access RRA services through a computer or a phone or visit an RRA agent for assistance. Those agents are private businesses that are contracted by RRA to assist citizens in using tax-related services.

Together these three cases make up a good set to reflect current e-government in Rwanda. These organizations are the largest ones involved in G2C and G2B services in Rwanda, and they

represent services accessed through the national portal (IREMBO) as well as outside of it. Figure 1 illustrates the relationships between the cases.

Figure 1: Cases illustration

5. Research methods

Data in this study was collected mainly through interviews with managers from the selected organizations who were responsible for planning, supporting, monitoring, and evaluating the development of regulations, policies, or technical practices related to IPP. We also conducted a survey to assess the privacy notice available on the IREMBO and also to verify the respondents' answers considering notice provided. In some cases we also verified the respondents' answers by checking the websites they referred to.

5. 1 Interviews

Structured interviews were conducted in connection with the chosen three cases (ROL, RRA, and RLMUA). Interviewees were selected by strategic sampling (Bryman, 2008) and included employees at management level who could answer the questions about implemented privacy practices. The respondents were responsible for planning, supporting, monitoring, and evaluating the development of any regulation, policy, or technical practices related to IP protection. We expected that their opinion and experience would help us to acquire a deep understanding of the situation. We conducted 11 face-to-face interviews with five employees of ROL, four of RRA, and two of RLMUA (Table 2). The interviews were conducted in October and November 2017,

and each interview lasted between 45 and 110 minutes. Interviews were voice recorded with interviewee permission.

Table 2: Interviewees

N ^o	Responsibilities	Organization
1	Legal Officer	ROL
2	Director IT operations	
3	Director of operations	
4	Operation manager (from a consulting firm)	
5	The staff in charge of content design	
6	Head of IT Unit	RRA
7	Head of the media division	
8	Head of business analysis division and e-tax project manager	
9	Electronic Single Windows project manager	
10	Director of MIS and IT support	RLMUA
11	Head of the legal department	

The interviews were guided by pre-arranged questions based on the definitions of matched privacy principles described in Section 3. To formulate the questions, we first identified the requirements that organizations need to meet to comply with each principle. We identified eleven requirements for principle of notice and awareness, six requirements for principle of access, three requirements for principle of user control, four requirements for principle of safeguard, accuracy and security, two requirements for storage limitation principle, five requirements for principle of enforcement and finally three requirements for principle of accountability. Second, we formulated one or more questions for each requirement to investigate whether the organizations' privacy practices comply with the requirement (Appendix 2). We identified 36 requirements. Some of the interview questions were yes/no-questions. For each of these, we prepared a set of follow-up questions so as to get an explanation of the reasons behind the yes or no.

5.2 Survey

The survey requested service users to assess the privacy notice available on the IREMBO platform. A privacy notice clarifies for users how the organization protects their IP by implemented IPP practices, i.e., how their data is being collected, the purpose of data collection, and the different uses of the data (AICPA & CICA, 2009; Al-Jamal & Abu-Shanab, 2015). By

comparing the users' answers from the survey with the interview answers, we could see whether the provided notice truly reflected the implemented IPP practices. We only considered the privacy notice on IREMBO (managed by ROL) as the other organizations (RRA and RLMUA) did not have any. The survey consisted of two parts: (1) demographic questions, and (2) close-ended questions to assess the IREMBO privacy notice. Following previous studies that examined privacy notices for e-government websites (Al-Jamal & Abu-Shanab, 2015; Nwaeze et al., 2017) we based our survey questions on privacy principles. We used the seven matched principles presented in Table 1 to formulate 14 assessment statements (see Appendix 4) that the participants were requested to agree or disagree to. Statements were for example "The privacy notice explains what data will be collected" and "The privacy notice clarifies why data will be collected". Apart from agreeing or disagreeing they could respond "not applicable" if they did not have any opinion or if they perceived the item as irrelevant. Those who responded not applicable were asked to explain their choice.

The survey was conducted during the same period as the interviews. It was distributed to 230 undergraduate students of the University of Rwanda, who acknowledged to be the users of IREMBO websites. 141 questionnaire were returned and usable, which yields a response rate of 69%. Of 141 respondents, 69% were men and 31% women. Most of them (93%) were aged 18-30, while 6% were aged 31-45. The group 46-55 had 1% respondents.

5.3 Data analysis

Interview recordings were transcribed for analysis. First, the interviews were analyzed separately for each organization, based on the seven matched principles and their related requirements. For each matched principle, we compared the answers provided by the different respondents belonging to the same organization. In cases when it was possible we also verified the respondents' answers. For instance, one respondents at RLMUA claimed that the organization uses the policy on the data protection (critical data protection) that could be found on the Ministry of ICT and Innovation website. However, when we checked the website did not contain any link to this law. In this way we could get a more comprehensive and objective view of the implemented IPP practices in each organization. Second, the answers concerning each principle were compared across the three studied organizations ROL, RRA and RLMUA. This was done for two reasons:

1) to see how the organizations collaborate to protect the users' privacy, especially regarding services offered through the national portal (IREMBO) and 2) to see if there are any common patterns in how the organizations comply with the seven matched principles and how they implement the IPP practices i.e. to see how the principles are met by e-government organizations in Rwanda.

The survey shows the users' view of the privacy notice provided at IREMBO platform. Survey data were analyzed using descriptive statistics. In order to understand how the users assessed the content of the privacy notice on IREMBO platform, frequency distributions were displayed for each one of the given statements in the questionnaire about group of questions. Within the next step, the survey data were compared to interviews data in order to affirm whether the privacy notice provides a correct description of the internal IPP practices. The interpretations of findings from both interviews and survey are fully discussed in next section. The findings from the survey were reported and discussed under the notice and awareness category. Indeed, survey assessed the content of the notice, and it pertains to notice and awareness category.

6. Findings

The section is structured according to the seven matched principles that were used to assess IPP practices at the three studied organizations. Table 3 shows a summary of the compliance with the principles across and within the assessed organizations (see Appendix 3 for details). The first column lists the matched principles used to assess the IPP practices in each organization. The other three columns report the studied organizations degree of compliance with each of these principles. Comply means that the organization's practices fully comply with the principle, not comply means that the organization's practices do not comply with the principle and partially comply means that they partially comply with the principle. Table 3 shows that compliance with the matched privacy principles generally is low in the studied organization. None of the organizations comply with all the seven matched principles. ROL complies with two of them (safeguard, accuracy security and the principle of and storage limitation) and partially complies with the principle of access and the principle of enforcement. RRA also complies with the principle of safeguard, accuracy security as well as the principle of and storage limitation, but only partially with the principle of enforcement. RLMUA complies only with the principle of safeguard, accuracy and security. Below we discuss each item in some detail.

Table 3: Compliance with information privacy principles by the assessed organizations

Principles	ROL	RRA	RLMUA
Notice and awareness	Not comply	Not comply	Not comply
Access	Partially comply	Not comply	Not comply
User control	Not comply	Not comply	Not comply
Safeguard, accuracy and security	Comply	Comply	Comply
Storage limitation	Comply	Comply	Not comply
Enforcement	Partially comply	Partially comply	Not comply
Accountability	Not comply	Not comply	Not comply

6.1 Notice and awareness

The notice and awareness principle concerns informing users about the use of collected information. It is obviously important that it correctly depicts actual internal privacy practices and that those practices are informed by policy, national or specific for the organization. None of the studied organizations met the requirements for this principle (see Appendix 2). None had a specific privacy policy and there was confusion regarding which national regulations should be used. At RRA, one respondent claimed that *“privacy protection is grounded in the tax law”*. However, another respondent stated that *“There is no policy to follow; I [handle personal information] following my common sense.”* At RLMUA, one respondent claimed that *“we apply the ministerial order on land registration for users’ information privacy protection.”* Another respondent claimed that the national data protection law is used: *“We use the policy on the data protection (critical data protection) [...] the link to this can be found on the ministry of ICT website”*. However, a visit on February 13, 2018, showed that the website does not contain any link to this law. All in all, the policy situation is unclear.

None of the organizations had a comprehensive and legitimate privacy notice. RRA and RLMUA did not have one at all. ROL provided a privacy notice at the IREMBO portal (<https://IREMBO.gov.rw/rolportal/web/rol>). However, as ROL does not have a privacy policy neither relies on any national or international policy to regulate privacy protection while handling users information, the source of its privacy notice is unidentifiable.

Even worse, the notice is misleading users. IREMBO is only a starting point for services pointing users to the organizations actually providing the service. A privacy notice at the service starting point may give users the impression that it is valid for the entire service, but this is not the case here. Says a ROL respondent: *“The privacy notice on IREMBO concerns information collected*

and held by ROL, not the information held by back-end organizations.” As RLMUA, a back-end organization who provides the actual services, does not have a privacy notice nor a policy, users are misled to believe that the notice on IREMBO is valid for the whole service.

Our survey to students shows that many were indeed misled. A majority answered YES for most of the survey assessment items (see figure 2), which implies that they thought the notice explains the IPP practices about their submitted information. But this is not true, as it does not address the information held and handled by back end offices, and this is not clarified. The problem of incoherent explanations in the notice is acknowledged by a ROL respondent: *The notice has a gap; it does not exactly explain what it concerns [...] We need to work with other agencies to find consensus approaches to protect users’ information.*” In other words, whatever explained in the notice is inappropriate as it does not clarify which kind of information it addresses and which parts of the service process are covered by it.

None of the organizations had assessed user awareness and comprehensibility of the privacy notice, and there was no understanding of the need for doing so. A ROL respondent said, *“There is no need of other strategies to ensure if the policy is known or not. It is available on the platform and that means is publicly known.”*

Figure 2: Frequency distribution for statements that used to assess the notice on IREMBO platform

The three organizations ask users to provide contact and geolocation information, so users might be aware of collected contact information. None of the organizations require information related to the computer (IP address, OS, etc.), interaction (historical search, browser behaviors, etc.), and sensitive issues (health status, criminal records, etc.). RRA requires sensitive information for some special cases (e.g., tax payment failures, frauds, evasion, etc.). Such information is collected with the permission of the owner or by law, and in the cases where the law intervenes, users are not necessarily informed.

ROL collects, stores, and shares users' financial information related to transactions users make when paying service fees. Users might be aware of that as they always submit that information when applying for services “” RRA *“collect[s] customers' financial information every year, we check income of business owners. We don't necessarily inform them. It is a matter of avoiding issues of fraud.”* RLMUA collects users' financial information related to the value of their plots. Users are not informed about the process of using and sharing such information.

The interviews, as well as visits to the organizations' websites, indicate that none of them use cookies. ROL has no strategies or mechanisms to inform users about how their personal information is used internally, what specific information would be used for in a specific context, or who the recipients of the shared personal information are. One ROL respondent noted, *“We don't inform customers. There is a matter of trust. I think citizens must understand [that] to inform them about internal activities can cause some vulnerabilities to [the] institution.”* He added, *“If we share information with other institutions, we don't inform customers.”* The same goes for RRA: *“RRA is a very big and complex organization...it will be not an easy task to communicate [with] customers on that.”* In some cases, RRA could inform users. For example, *“[If] a person fails to pay back a bank loan and is taken into court, the court may investigate his registered properties (e.g., cars). In that case, the person would be informed that the court is searching for information regarding his/her properties.”* Neither does RLMUA have a specific strategy to inform users about how their information is used internally, which information will be used for a specific context, and who will be the recipient of their information.

6.2 Access

The interviews indicate that none of the three organizations have an agreement with third parties in term of protecting privacy of the accessed users' personal information. ROL is the only organization that has an agreement that includes affiliated organizations. The Build-Operate-Transfer (BOT) agreement between ROL and the Government of Rwanda defines the role of ROL, government organizations, and other third-party contractors including banks and telecommunication companies, in processing applications, but it only partially covers privacy issues. RRA applies the tax law as well as the law on electronic transactions to identify third parties who can access users' information. In addition to that, the customs department can use

World Trade Organization (WTO) and World Customs Organization (WCO) standards for such practices. All these laws only partially cover privacy-related issues. RLMUA does not have any policy or strategy that identified third parties and organization contractors.

Neither ROL has a policy nor practices concerning which employees or employee categories have access to users' information. One ROL respondent explained, *"As we are in the same service, every employee can access any data whenever required."* At RRA and RLMUA, each employee accesses users' information based on his or her duties. At RRA, internal documents describe the processes and procedures for information flows inside the organization. RLMUA does not have such documents.

ROL and RRA do not ask users for consent before sharing their personal information. An RRA respondent suggests that consent might not be legal, *"In practice, I doubt that RRA can allow customers to give consent on sharing information."* RLMUA sometimes asks users for consent before sharing their information, depending on the type of information and who is requesting. One respondent explains, *"If you need information about a plot, we always ask the owner consent before giving this information. For public institutions, the appropriate units assess their requests and answers them without user consent."*

6.3 Users' control

This principle concerns the users' options to adjust the privacy settings, to access their collected personal information, to anonymize or delete their personal information. Interviews indicate that none of the organizations allow users to adjust privacy settings. An ROL respondent suggests that *"it is not necessary. We are not commercial site...we record and keep information that is needed to process users' applications."* ROL users can request to have certain information deleted. ROL users can only view the history of their applications via IREMBO. RRA service users can access some of their information, *"for example tax information in local government is available. Customers can access and revise it."* RLMUA service users can only view the process of their applications, not anonymize or delete any information or adjust privacy settings.

6.4 Safeguard, accuracy and security

Two of three assessed organizations, ROL and RLMUA work with the National Identification Agency (NIDA) and the National Prosecution Agency to ensure the accuracy of user information. RRA does not have mechanisms to ensure user information accuracy. All three organizations reserve the right to disclose personal information to comply with laws, protect from crime, or defend its own rights. An RLMUA respondent explained, *“Let’s say that a customer accuses the institution to offer poor services or treat customers’ applications in [the] wrong way. In that case, we publish all the information to protect the institution’s reputation.”* All respondents claimed that the three organizations have appropriate security means such as encryptions tools, VPN, IDS, firewalls, and antivirus.

6.5 Storage limitation

Storage limitation concerns management of users’ information when their account is closed and if there is a time-limit for users’ personal information retention.

RRA has strategies to manage user information when their accounts are closed. *“When closing customers’ accounts, there are a lot of criteria to follow, and these are in the tax registry policy.”* An ROL respondent stated, *“We don’t close accounts, our business model specifies that user accounts must not be closed”*. RLMUA lacks exit strategies.

ROL has regulations for keeping and deleting user information. *“We need to keep information for five years [...] information older than five cannot be request[ed], this is specified in the BOT.”* At RRA, *“we are supposed to keep data for 10 years. This is specified in the tax law.”* As for RLMUA, there is no defined limit for data retention.

6.6 Enforcement

The enforcement principle concerns how information privacy protection principles are formally established in regulations.

At IREMBO and RRA, users can call the call center, email, and use live chat to ask about privacy concerns. RLMUA does not have any such options for users to submit their complaints or privacy

concerns. Only ROL has a privacy disclaimer on the website. Only ROL has a privacy seal with Entrust Ltd. None of the organizations has any specific agency for privacy-violation issues like for other types of complaints where users can call other organizations who generally monitor operations, such as RURA (Rwanda Utility Regulatory Authority), RGB (Rwanda Governance Board) or the Prosecution Office.

6.7 Accountability

This principle involves organizations' engagement, transparency and responsibilities in protecting users' information.

None of the three organizations has a privacy protection officer. Neither do they arrange specific training concerning privacy protection. An ROL respondent says, *"Indeed, we don't need that. Why would we plan training on privacy when there has been no harm done?"* The ROL Senior Management Board does not consider privacy protection an important matter. One respondent says, *"We have to understand what privacy means first of all. We have to understand our context first of all. Privacy [definitions] differs between different lawyers."* Another ROL respondent said, *"We are not really concerned with privacy protection. Note that our major role is to facilitate government agencies to communicate with citizens. The privacy protection aspect must more [be] taken within institutions that are keeping people's data".* RRA and RLMUA respondents generally stated that the role of senior management is based on establishing policies, sensitizing the employees to obey existing laws and strategies, and enforcing. However, there is no specific agenda for privacy. One RRA respondent noted that *"following this discussion, I realize that we still have a lot to do to protect privacy. We have to establish a clear plan for collecting and sharing customers' information."*

7. Discussion of findings and implications

Based on our empirical results, we want to highlight four important implications for research and practice.

First, being among the few that study privacy and e-government in an African LDC context our study adds to general knowledge of privacy protection in e-government in that context. It contributes to research by establishing the current situation regarding information privacy

protection in e-government in one specific African LDC by collecting evidence of compliance by government organizations with international privacy principles. Research with a focus on Africa – the world’s second-largest continent with 54 countries – is almost non-existent, not only concerning information privacy but in information systems research in general. E-services is an important application domain, rapidly growing in Africa, which presents important areas for potential research (Mbarika & Byrd, 2005). Although privacy could be context-specific (Xu et al., 2011), e-service is by nature a trans-border activity. Many e-government activities concern trans-border activities, e.g. import, travel, and export, and all such activities become easier if the legal frameworks regarding information handling are similar in all countries involved. As concerns privacy, there is also a human rights factor – for example, the UN, consider that citizens across the globe should enjoy right to privacy in the digital age (UN, n.d.).

Second, our study is among very few studies (Nwaeze et al., 2017; Verkijika & De Wet, 2018) assessing IPP practices in e-government in Africa. Consistent with previous studies we found that Rwanda still has a long way to go to establish effective IP practices (Makulilo, 2015). Our study differs from previous studies (Nwaeze et al., 2017; Verkijika & De Wet, 2018) in that we focus on actions inside the organizations (e-government service providers) while previous studies assess IPP principles visible on the organizations’ websites i.e. privacy notice. As our study shows, privacy notices visible on a website may be misleading and not always correspond to IPP practices within an organization. Therefore, this study contributes to increased understanding of how privacy practices are carried out within e-government organizations in an African LDC context.

Third, this study contributes to existing knowledge by providing a set of matched IP principles derived from five sets of well-known international principles: OECD, FIP, ISO, GAP, GDPR. Several previous studies (Al-Jamal & Abu-Shanab, 2015; Marotta-Wurgler, 2016; Nwaeze et al., 2017; Stanaland & Lwin, 2013) have used international principles as an assessment tool, however because different sets of IP principles, have considerable overlaps and sometimes use different terms referring to similar issues (Al-Jamal & Abu-Shanab, 2015). To cover all important aspects but avoid redundancy of issues we matched five sets of the most used international principles to a new set which then is more representative for international best practice than any one single set alone.

Fourth, this study is the first to assess the IPP practices in e-government in Rwanda and as such contributes to better understanding of current privacy protection practices Rwanda and by highlighting the problems in existing IPP practices will contribute to the development of robust IPP practices in e-government in Rwanda. As Table 2 shows, only three out of the seven principles are, to some extent, met—*Safeguard, security and accuracy, Storage limitation, and Enforcement*. Four are not at all met—*Notice and awareness, Access, User control, and Accountability*. On this basis, there is reason to call into question the efficacy of existing IPP practices and their general potential effect in ensuring e-government users' privacy protection in Rwanda.

The study also displays a lack of dedicated privacy policy and uncertainty about how other relevant policy/law/regulation can and should be used to guide the privacy practices. This is consistent with previous studies (e.g. Botha & Grobler 2017 and Yilma 2017) who put Rwanda on the list of the countries that need to enact comprehensive national privacy regulation and principles. National regulation not only facilitates effective organizational practices, but also gives users a ground to believe that organizations will protect their information, which increases their trust in e-services (Xu et al., 2012). The lack of the privacy policy also implies the need of implementing organizational privacy self-regulation to cater for the gaps in existing legislation that has some bearing on privacy. Borena et al (2015) argue that given the positive contribution of self-regulation, which is driving innovation, self-regulation in Africa should be considered as an effective practice for IP protection.

Contrary to some previous research claiming that development of technological solutions to protect privacy does not seem viable in African countries (Borena et al., 2015) our study shows that the assessed organizations offer significant attention to technological practices. This is in fact the most developed area; all assessed organizations have appropriate security means such as encryptions tools, VPN, IDS, firewalls, and antivirus tools.

Our study also shows that there is a need for enhancing awareness and enforcement of existing laws and regulations. Although Rwanda still lacks a dedicated national privacy regulation there exists a set of other regulations that at least to some part could guide information privacy protection (Nsengimana, 2017), but in the organizations we assessed there were confusion as to which regulation should be used, and how. It is important to note that awareness of these

regulations concerns not only the service providers; it is also an important tool to increase users' trust in e-services (Alasem, 2015).

Two of the three assessed organizations lack a privacy notice and the third organization provides a misleading one which does not reflect the existing IPP practices. This is a serious problem since according to e-government best practices a readable and comprehensive privacy notice is one of the most important criteria for government websites (Nyakwende & Mazari, 2012).

The study also shows that there is a need for structured collaboration among government organizations, in particular those which offer services that are accessed through the national portal (IREMBO) regarding ensuring the privacy of users' information. Coordination of initiatives and collaboration among entities can be another precondition for developing adequate practices for IPP (Karokola, 2012).

Finally, our findings suggest that there is a need for enhancing users' ability to control their interactions with e-government. Most of the IPP principles concerning individual's privacy are not met by the service providers we studied. Users are not informed about existing IPP practices, they have no control over collection and processing of their personal data, and accountability is low. The element of control of individuals' personal information is embedded in most IP definitions (Xu et al., 2012), and this explains the salient link between individuals' control and IP. Particularly, in the context of e-service, the right to privacy is the right to control the use of personal information that is disclosed to others (Alasem, 2015).

8. Conclusion

This study assesses the status of existing privacy practices in e-government in Rwanda. A set of seven matched international privacy principles was used as assessment baseline. Three cases were studied — RwandaOnline (ROL), Rwanda Revenue Authority (RRA), and Rwanda Land Management and Use Agency (RLMUA). The findings show that the assessed organizations only partially comply with those principles. This result implies that several things need to be done. There is a need to establish national privacy regulation or principles so as to make up a clear foundation for privacy protection practices in e-government. Until this is done, there is a need to enhance awareness of already existing policies and regulations related to privacy protection; at least they provide some ground for protective measures. There is also a need for structured

collaboration among government organizations toward privacy protection many services involve more than one organization and both practices and information to users about practices must be consistent across the whole service process.

In order to make this happen, e-government project leaders and managers of organizations providing e-government services in Rwanda should be educated in the current and forthcoming relevant legislation and instructed to make privacy protection a priority during service development. User trust is a key success factor for e-government development and designing privacy protection measures in parallel to systems development and implementation is the quickest way to improvement. The results also call upon the government organizations in Rwanda to not limit privacy protection to technical aspects as the most prevalent factors for e-government failure in developing countries are linked to lack of non-technical aspects such as IP legislations and to the in which ways information handling in service processes is organized (Miyungire & Yonazi, 2012; Nyakwende & Mazari, 2012).

Although this mainly qualitative study cannot be directly generalized to all African LDCs, clearly many other African LDCs are in situations similar to that of Rwanda so at least this study can serve as an inspiration for them. African LDCs have a lot in common, such as poor infrastructure, low development of human and institutional resources that make them more vulnerable to privacy violation.

For future research, we suggest more studies investing privacy compliance in African LDCs. Assessment of privacy compliance may serve as a baseline to ensure conformance with applicable regulations and principles for privacy, determine the privacy threats, and identify alternatives to mitigate those threats.

Reference

- Abu-Shanab, E. (2014). Antecedents of trust in e-government services: an empirical test in Jordan. *Transforming Government: People, Process and Policy*, 8(2), 283–308. <http://doi.org/doi:10.1108/TG-08-2013-0026>
- AICPA, & CICA. (2009). *Generally Accepted Privacy Principles*. Retrieved from http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/DownloadableDocuments/GAPP_PRAC_0909.pdf

- AICPA, & CICA. (2011). *Privacy Maturity Model*.
- Akkaya, C., Wolf, P., & Krcmar, H. (2012). Factors Influencing Citizen Adoption of E-Government Services: A Cross-Cultural Comparison (Research in Progress). *Proceedings of the 45th Hawaii International Conference on System Sciences (HICSS-45)*. Maui, HI, USA: IEEE. Retrieved from <http://www.computer.org/csdl/proceedings/hicss/2012/4525/00/4525c531-abs.html>
- Al-Jamal, M., & Abu-Shanab, E. (2015). Privacy policy of e-government websites: An itemized checklist proposed and tested. *Management Research and Practice*, 7(3), 80–95. Retrieved from http://oru.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMw1V3da8IwEA%7B_%7DTh7GXsU%7B_%7D24SAw2EvpaK2t6WAPndbNoba0zrG9SGwjE6aC04f997uYpHYd-L6nlqaE0N%7B_%7DI7nL93R1CVvXW0As6YURHtYSZdTYmY7ChDjMop7HVSArmJaU8lbyTtcKG02mRaEOnVx2k5gtOI%7B_%7DsvAIdRe-A13rQw6LT
- Alasem, A. N. (2015). Privacy and eGovernment in Saudi Arabia. In *World Congress on Engineering and Computer Science* (Vol. II, pp. 21–24).
- Argyarakis, J., Gritzalis, S., & Kioulafas, C. (2003). Privacy Enhancing Technologies: A Review. (R. Traunmüller, Ed.), *Electronic Government: Proceedings of the 2nd [IFIP WG 8.5] International Conference, EGOV 2003*. Prague, Czech Republic. Retrieved from <http://www.springerlink.com/openurl.asp?genre=article&id=W19UAWJ7V3H9EGQ0>
- Belanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *Journal of Strategic Information Systems* 1, 17, 165–176. <http://doi.org/10.1016/j.jsis.2007.12.002>
- Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information system. *MIS Quarterly*, 35(4), 1–36.
- Borena, B., Bélanger, F., & Ejigu, D. (2015). Informatiopracton Privacy Protection Practices in Africa: A review trough the lens on critical social theory. In *48th Hawaii International Conference on System Sciences* (pp. 3490–3497).
- Botha, J., & Grobler, M. (2017). A High-Level Comparison between the South African Protection of Personal Information Act and International Data Protection Laws A High-Level Comparison between the South African Protection of Personal Information Act and

- International Data Protection Laws. In *The 12th International Conference on Cyber Warfare and Security (ICCWS)*. Ohio, USA.
- Bryman, A. (2008). *Social Research Methods*. Oxford: Oxford University Press.
- Chen, Y.-C., & Hsieh, T.-C. (2014). Big Data for Digital Government: Opportunities, Challenges, and Strategies. *International Journal of Public Administration in the Digital Age*, 1(1), 1–14.
- Chua, H. N., Herbland, A., Wong, S. F., & Chang, Y. (2017). Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. *Telematics and Informatics*, 34(4), 157–170. <http://doi.org/10.1016/j.tele.2017.01.008>
- CIGI & Ipsos. (2018). 2018 CIGI-Ipsos Global Survey on Internet Security and Trust. Retrieved from <https://www.cigionline.org/internet-survey-2018>
- Culnan, M. ., & Bies, J. . (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, 59(2), 323–342.
- Dayarathna, R. (2013). *Discovering Constructs and Dimensions for Information Privacy Metrics*. Retrieved from <http://www.diva-portal.org/smash/get/diva2:617312/FULLTEXT02.pdf>
- Heurix, J., Zimmermann, P., Neubauer, T., & Fenz, S. (2015). A taxonomy for privacy enhancing technologies. *Computers & Security*, 53, 1–17. <http://doi.org/http://dx.doi.org/10.1016/j.cose.2015.05.002>
- Holden, S. H., Norris, D. F., & Fletcher, P. D. (2003). Electronic Government at the Grass Roots: Contemporary Evidence and Future Trends. *Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS-36)*. Island of Hawaii (Big Island): Computer Society Press. Retrieved from <http://csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/proceedings/hicss/&to c=comp/proceedings/hicss/2003/1874/05/1874toc.xml&DOI=10.1109/HICSS.2003.1174305>
- Human Rights Committee. (2015). *The Right to Privacy in Rwanda*. Retrieved from <https://www.privacyinternational.org/sites/default/files/PI Rwanda submission.pdf>
- Karokola, G. R. (2012). *A Framework for Securing e-Government Services The Case of Tanzania*.

- Retrieved from <http://www.diva-portal.org/smash/get/diva2:557279/FULLTEXT04.pdf>
- Kim, G.-H., Trimi, S., & Chung, J.-H. (2014). Big-data applications in the government sector. *Communications of the ACM*, 57(3), 78–85. <http://doi.org/10.1145/2500873>
- Libaque-Sáenz, C. F., Wong, S. F., Chang, Y., Ha, Y. W., & Park, M. C. (2016). Understanding antecedents to perceived information risks: An empirical study of the Korean telecommunications market. *Information Development*, 32(1), 91–106. <http://doi.org/10.1177/0266666913516884>
- Makulilo, A. B. (2012). Privacy and data protection in Africa: a state of the art. *International Data Privacy Law*, 2(3), 163–178. <http://doi.org/10.1093/idpl/ips014>
- Makulilo, A. B. (2015). Myth and reality of harmonisation of data privacy policies in Africa. *Computer Law & Security Review*, 31(1), 78–89. <http://doi.org/10.1016/j.clsr.2014.11.005>
- Marotta-Wurgler, F. (2016). *Understanding Privacy Policies: Content, Self-Regulation, and Markets* (16-18). <http://doi.org/10.2139/ssrn.2736513>
- Maumbe, B. M., Owei, V., & Alexander, H. (2008). Questioning the pace and pathway of e-government development in Africa: A case study of South Africa's Cape Gateway project . *Government Information Quarterly*, 25(4), 757–777.
- Mbarika, V. W. a, & Byrd, T. A. (2005). The Neglected Continent of IS Research : A Research Agenda for Sub-Saharan Africa. *Journal of the Association for Information Systems*, 6(5), 130–170. <http://doi.org/10.1177/1094670509357611>
- McDonagh, M. (2002). E-Government in Australia: the Challenge to Privacy of Personal Information. *International Journal of Law and Information Technology*, 10(3), 327–343. Retrieved from <http://proquest.umi.com/pqdweb?did=954870581&Fmt=7&clientId=8991&RQT=309&VName=PQD>
- Ministry of Natural Resource. (2012). *Land Administration Procedures*. Retrieved from http://rnra.rw/fileadmin/fileadmin/user_upload/documents/LAS_Manual.pdf%0Ahttps://www.dropbox.com/s/4jky43vqakopj8r/LAS_Manual.pdf?dl=0
- Miyungire, G., & Yonazi, J. (2012). Identifying Citizen-Demanded eGovernment Services in

- Tanzania. In *12th European Conference on eGovernment (ECEG 2012)* (pp. 447–453). Barcelona, Spain.
- Murphy, A. R., Reddy, M. C., & Xu, H. (2014). Privacy practices in collaborative environments: A study of emergency department staff. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing - CSCW '14* (pp. 269–282). <http://doi.org/10.1145/2531602.2531643>
- Mwangi, W. (2006). The Social Relations of e-Government Diffusion in Developing Countries: The Case of Rwanda. *7th Annual International Conference on Digital Government Research (Dg.o 2006)*. San Diego: Digital Government Research Center.
- Nkwe, N. (2012). E-government: challenges and opportunities in Botswana. *International Journal of Humanities and Social Science*, 2(17), 39–48. Retrieved from http://www.ijhssnet.com/journals/Vol_2_No_17_September_2012/5.pdf
- Nsengimana, J. P. (2017). Reflections upon periclitations in privacy: perspectives from Rwanda's digital transformation. *Health and Technology*, 7(4), 377–388. <http://doi.org/10.1007/s12553-017-0196-0>
- Nwaeze, A. C., Zavarsky, P., & Ruhl, R. (2017). Compliance Evaluation of Information Privacy Protection in e-Government Systems in Anglophone West Africa using ISO / IEC 29100 : 2011. In *The Twelfth International Conference on Digital Information Management (ICDIM 2017)* (pp. 98–102).
- Nyakwende, E., & Mazari, A. Al. (2012). Factors Affecting the Development of e-Government in Saudi Arabia. (A. Kö, C. Leitner, H. Leitold, & A. Prosser, Eds.), *Advancing Democracy, Government and Governance: Proceedings of the Joint International Conference on Electronic Government and the Information Systems Perspective, and Electronic Democracy (EGOVIS/EDEM 2012)*. Vienna, Austria. Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-32701-8_3
- Oetzel, M. C., & Spiekermann, S. (2014). A systematic methodology for privacy impact assessments: A design science approach. *European Journal of Information Systems*, 23(2), 126–150. <http://doi.org/10.1057/ejis.2013.18>
- Pelkola, D. (2012). A framework for managing privacy-enhancing technology. *IEEE Software*,

- 29(3), 45–49. <http://doi.org/10.1109/MS.2012.47>
- RLMUA. (2017). Rwanda Land Management and Use Authority. Retrieved from <http://www.rlma.rw/about-us/objectives/>
- Rwanda. (2012). Rwanda vision 2020. Revised in 2012, 1–40. Retrieved from http://www.minecofin.gov.rw/fileadmin/General/Vision_2020/Vision-2020.pdf
- Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *Management Information Systems Quarterly*, 20(2), 167–196. <http://doi.org/10.2307/249477>
- Solove, D. J. (2006). Taxonomy of Privacy. *University of Pennsylvania Law Review*, (335), 335–409.
- Stanaland, A. J. S., & Lwin, M. O. (2013). Online Privacy Practices: Advances in China. *Journal of International Business Research*, 12(2), 33–47.
- Stewart, K., Kane, G. C., & Storey, V. C. (2006). Compliance to the fair information practices : How are the Fortune 500 handling online privacy disclosures ? *Information & Management*, 43, 805–820. <http://doi.org/10.1016/j.im.2006.07.003>
- The Republic of Rwanda. (n.d.). e-Services. Retrieved from <https://irembo.gov.rw/rolportal/en/eservice-by-name>
- The Republic of Rwanda. The constitution of the Republic of Rwanda of 2003 revised in 2015 (2015). Retrieved from http://www.parliament.gov.rw/fileadmin/Bills_CD/THE_CONSTITUTION_OF_THE_REPUBLIC_OF_RWANDA_OF_2003_REVISED_IN_2015.pdf
- The Republic of Rwanda. (2016). Law governing Information and Communication Technologies. Retrieved from http://www.rura.rw/fileadmin/docs/Law_governing_Information_and_Communication_Technologies_Levy_on_petron__27_06_2016.pdf
- UN. (n.d.). The Right to Privacy in the Digital Age. Retrieved October 11, 2018, from <https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx>
- UNDESA. (2018). 2018 E-Government Survey. Retrieved from

<https://publicadministration.un.org/en/research/un-e-government-surveys>

- UNPAN. (2016). Rwanda: Citizens Commend E-Government Services. Retrieved from <http://www.unpan.org/Library/MajorPublications/UNEGovernmentSurvey/PublicEGovernanceSurveyintheNews/tabid/651/mctl/ArticleView/ModuleId/1555/articleId/50072/Rwanda-Citizens-Commend-EGovernment-Services.aspx>
- Verkijika, S. F., & De Wet, L. (2018). A usability assessment of e-government websites in Sub-Saharan Africa. *International Journal of Information Management*, 39, 20–29. <http://doi.org/10.1016/j.ijinfomgt.2017.11.003>
- Welch, E. W., Feeney, M. K., & Park, C. H. (2016). Determinants of data sharing in U.S. city governments. *Government Information Quarterly*, 33(3), 393–403. <http://doi.org/10.1016/j.giq.2016.07.002>
- World Bank. (2016). DataBank. Retrieved from <https://data.worldbank.org/country/rwanda>
- Wright, D., & Raab, C. (2014). Privacy principles, risks and harms. *International Review of Law, Computers & Technology*, 28(3), 277–298. <http://doi.org/10.1080/13600869.2014.913874>
- Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior*, 28(3), 889–897. <http://doi.org/10.1016/j.chb.2011.12.008>
- Xu, H., Bagby, J. W., & Melonas, T. R. (2009). Regulating privacy in wireless advertising messaging: FIPP compliance by policy vs. by design. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 5672 LNCS, pp. 19–36). http://doi.org/10.1007/978-3-642-03168-7_2
- Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information Privacy Concerns : Linking Individual Perceptions with Institutional Privacy Assurances Information Privacy Concerns : Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association for Information Systems*, 12(12), 798–824.
- Xu, H., Teo, H., Tan, B. C. Y., & Agarwal, R. (2012). Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services. *Information Systems Research*, 23(4), 1342–1363.

<http://doi.org/10.1287/isre.1120.0416>

Yilma, K. M. (2017). The Quest for Information Privacy in Africa: A Review Essay. *Journal of Information Policy*, 7, 111–119. Retrieved from <https://www.jstor.org/stable/pdf/10.5325/jinfopoli.7.2017.0111.pdf?refreqid=search%3A89c9455655e04254dec3f155a02b3ce5>