Privacy and eGovernment in Saudi Arabia

Abdulrahman N. ALASEM

***Abstract*— This study assessed the inclusion of visible privacy statements on Saudi government websites as a measure of Saudi eGovernment's management of privacy and security concerns and surveyed Saudi eGovernment users' perspectives on relevant privacy issues. 174 government websites, or 100% of the websites listed in the Saudi National eGovernment Portal directory, were reviewed. Of these, 44% provided a visible privacy statement, 39% did not present a privacy statement, and 17% could not be accessed. Furthermore, the websites that did present a privacy statement used various terms for the statements, which is inconsistent with the fundamental principles of government website design. Based on related studies, a questionnaire was then developed to assess eGovernment users' level of privacy awareness. Of the 53 questionnaire respondents, 44 were eGovernment users. These users, both male and female, generally demonstrated limited knowledge of their privacy rights. However, they shared similar concerns about sharing their personal information, with male users demonstrating a higher level of concern. To some extent, the users felt unsafe providing their personal information online. Finally, to improve the Saudi eGovernment project, Saudi Arabia should adopt a data protection act and enforce standard terminology for privacy statements across all Saudi government websites.**

***Index Terms*— eGovernment, Privacy, Saudi Arabia eGovernment, eGovernment non-technical barriers.**

I. INTRODUCTION

The term "eGovernment" is widely used to describe the use of information and communication technology (ICT) in the public sector. eGovernment applications help governments increase transparency, improve government services, and save money. However, the number of successful eGovernment initiatives globally is low, particularly in developing countries, as various ICT infrastructure, political, social, and organizational factors can lead to a partial or total failure of eGovernment applications.

In developing countries, especially Arab countries, the most prevalent factors of eGovernment failure are linked to non-technical issues. In the Saudi context, several studies have shown that two types of trust are critical in Saudi eCommerce and eGovernment success: Internet trust and government trust. For instance, a 2007 CITC report found that 29% of Saudi participants believed using the Internet for shopping was not safe [1]. Likewise, Sait et al. found a positive relationship between strong support of eCommerce adoption and an emphasis on privacy and security issues among Saudi users [2]. Based on similar findings, Alharby identified privacy and security as two of the greatest barriers to Saudi eCommerce adoption [3]. With respect to eGovernment, the majority of Saudi Internet users Alotaibi surveyed indicated concern about privacy and security in online government applications [4]. Users' level of trust can also vary from government agency to agency based on personal experience or stories reported by family, friends, or the media.

Website design can help improve users' trust. However, Alhazani found that only four of the 22 government ministries she reviewed, which were primarily Saudi ministries, provided a visible privacy policy statement on their websites [5]. In eGovernment website design best practices, a visible privacy statement is one of the most important evaluation criteria for government websites. For example, in the UK, the *Guidelines for UK government websites*, the *Quality Framework for UK Government Website Design*, and the *Illustrated handbook for Web management teams* all note that government websites must provide a visible privacy statement [6, 7, and 8]. In Australia, the *ACT Government Website Guidelines,* published by the Office of Information Technology and Multimedia, and the "Implementing an Effective Website Search" guidelines, published by the Australian Government Information Management Office, both indicate that every government website must have a visible privacy statement [9, 10]. Likewise, www.usability.gov, which is a guide for developing usable and useful US government websites, states that a visible privacy statement is mandatory for all US government websites [11]. With these examples in mind, the present study aimed to assess Saudi government websites in terms of providing visible privacy statements and generate a profile of eGovernment users in Saudi Arabia to identify major concerns related to privacy issues.

II. LITERATURE REVIEW

Privacy and security are typically discussed together under the term "user trust," which the literature approaches as a technical barrier [12]. In the context of eGovernment, users' perspectives on government privacy practice and government website security are considered non-technical barriers [13]. In this case, as Al-Busaidy and Weerakkody have noted, trust refers to a user's belief in the security and privacy afforded in electronic transactions on official government websites [14], and privacy refers to "credible government protection" of citizens' personal information [15]. In the context of eGovernment and eCommerce, the right to privacy is the right to control the use of personal information that is disclosed to others [16].

As they are among the most significant barriers to eGovernment, much has been written on user beliefs in privacy and security [15, 17, 16, 18, and 19]. For example, in its annual global report on online eGovernment, Taylor Nelson Sofres found that 23% of eGovernment users felt unsafe providing personal information online; this figure increased to 25% in 2003 [20]. Exploring these user concerns, a 2007 AGIMO study on Australians' use and

Information Studies Department, College of Computer and Information Sciences, Al Imam Mohammad Ibn Saud Islamic University, P.O. Box 5701, Riyadh11432, Saudi Arabia. email: a.alasem@ccis.imamu.edu.sa

satisfaction with eGovernment services found that government agencies could encourage up to 6% of Internet users to use eGovernment services by addressing privacy issues and providing visible privacy statements [21].

Such privacy concerns are subject to not only individuals but also businesses. For example, in Adeshara et al.'s study, 21% of participating small and medium sized enterprises (SMEs) in the UK admitted they were most concerned about violations of privacy when using eGovernment services, whereas 28% were most concerned about transaction security [22]. These results support Culnan and Armstrong's argument that US citizens are more likely to disclose personal information if they are aware of the agency's privacy practices [23].

Clearly, privacy and security issues are significant for eGovernment users in countries such as the US and the UK that have been supporting privacy rights since the 1960s or early 1970s [24]. Thus, many developed countries have adopted data protection policies. For example, the UK adopted the Data Protection Act of 1998, replacing the Data Protection Act of 1984 and the Access to Personal Files Act of 1987. The 1998 act contains eight principles covering the manual and automatic processing of personal data. These principles are based on three concepts: purpose of collecting personal data, fairness to be collected for legitimate purposes and transparency, and the right of users to have which data collected [24].

In some parts of the world, however, privacy is considered a Western concept [25], perhaps because Western societies have a long history of democracy and the passage of legislation concerning privacy. Although many regions around the world do not share this same democratic history, these regions now have many things in common with Western societies because of the development of ICT and the advent of the Internet. Various concepts that originated in developed countries have become global concepts, including the concept of privacy. Thus, in several developing countries, what was previously of no concern has become a necessity. For example, in a study on eGovernment in Jordan, Hussein found citizens had concerns about privacy; in particular, the Jordanian government collects a large amount of personal information about its citizens, and this information could be used inappropriately [26]. Similarly, in Bahrain, 82% of Bahraini respondents who did not participate in eCommerce refrained from doing so due to non-technical barriers, including privacy concerns [27].

III. . Methodology

This study is descriptive in natural, and two methods were adopted. First, the 174 government websites listed in the Saudi National eGovernment Portal http://www.saudi.gov.sa/ were checked. This was done by accessing the government agency directory in the portal, which is divided into 14 sections, each containing websites of numerous government agencies. This directory contains almost all the various types of government websites. Next was to access each site's interface to see if the agency has a visible privacy statement which is a legal statement that informs the website's users as to how the personal information they provide will be used, disclosed, and managed. Based on the finding of the websites checked and related studies, a questionnaire was developed in order to meet the aim and objectives of the study regarding privacy considerations of expected users of eGovernemnt. The questionnaire is comprised of different types of questions, such as those requiring yes/no responses, multiple choice responses and Likert-scale responses divided into two sections: section one is about personal information and contains five questions. Section two is about the eGovernment users participants' opinions regarding privacy issues when using Saudi government websites, and this section contains six questions. The questionnaire was distributed online, and SPSS 15.5 was used to analysis the data. Frequencies and basic techniques had been adopted. Finally, the data used in this study for both methods were collected between April 1 and 20, 2015.

IV. Result and discussion

The results concerning the provision of visible privacy statements on the 174 Saudi government websites reviewed were generally disappointing, especially considering Saudi Arabia established its eGovernment project in 2005. Only 44% (76) of the websites provided a visible privacy statement; 39% (68) failed to present a privacy statement, and the remaining 17% (30) could not be accessed, as either the website was no longer active or the portal directory contained a broken or invalid link.

Furthermore, no standard terminology was used across the websites to identify privacy statements. In English, "privacy statement" is the standard term used to inform users how their personal information will be used, disclosed, and managed; however, in Arabic, one can use several terms to denote the same concept of privacy. In this case, approximately 70% of the websites with privacy statements used the term "privacy statement"; however, the remaining websites used a range of terminology for their statements. This inconsistency is contrary to government website design best practices, as outlined in the introduction.

Finally, the privacy statements also varied from site to site. This variation reflects Saudi Arabia's current lack of a specific data protection act. Thus, the privacy statements provided on the websites were developed based on several different laws, specifically, al-Shari'ah principles (Al-Fawzan and Elsayed, 2012).

In terms of the results of the questionnaire, Table 1 presents the participants' demographic characteristics.

Of the 31 male participants, 28 had used government websites. Of the 22 female participants, 16 had used government websites. For the purpose of this study, non-users were excluded from the analysis.

Regarding the results for the second section of the questionnaire, there was a slight difference between male and female participants concerning their knowledge of privacy rights when accessing government websites, with a mean value of 2.21 and 2.56, respectively. In terms of the participants' privacy concerns when using government websites (e.g., registration or transactions via government

ISBN: 978-988-14047-2-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

websites), the male participants indicated a higher level of concern, with a mean value of 4.18 and 3.88, respectively, for males and females. However, many participants admitted they rarely reviewed a government website's privacy statement before providing their personal information; specifically, when asked how often they checked this statement, 4% indicated "always," 32% chose "often," 39% answered "rarely," and 25% selected "never." At the same time, the majority (69% of male participants and 54% of female participants) felt unsafe providing their personal information on government websites.

Table 1:Demographic characteristics of the participants

	eGov Users		Non Users	
	N	*%*	*N*	*%*
Gender				
Male	28	90	3	10
Female	16	73	6	27
Demographic characteristics of the eGov users participants				
Age				
20-29	32		73	
30-39	12		27	
40-49	0		0	
Over 50	0		0	
Education level				
Basic	0		0	
Secondary	10		23	
Undergraduate	34		77	
Postgraduate	0		0	
Internet experience				
Year >	0		0	
1-2	0		0	
3 <	44		100	

Regarding their perspectives on the amount of personal information being collected by government websites, the majority (83% of male participants and 77% of female participants) felt government websites asked for a large amount of personal information, even for basic tasks. For example, to obtain general information via the "Contact Us" eForm on some government websites, users must provide their name, phone number, email, and National ID number, as seen in Figure 1.

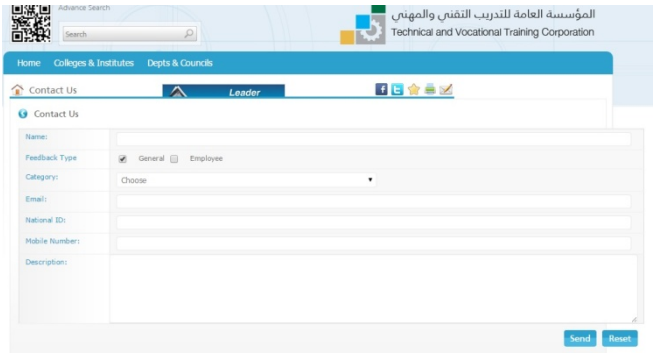

Fig. 1 Technical and Vocational Training Corporation's contact form.

V. Conclusion

As the literature has demonstrated, privacy is one of the most important factors affecting the adoption and use of eGovernment services. Any maladministration of privacy and security concerns can lead to a partial or total failure of eGovernment initiatives. In developing countries, the situation is even more complex as these countries have not yet developed relevant policies and laws. Clearly, eGovernment is not just about utilizing ICT in the public sector; it is about changing the way in which government works. Thus, governments should devote just as must attention to non-technical barriers, including privacy, as they do to technical aspects.

In the specific Saudi context, the current government websites are disappointing with respect to addressing users' privacy and security concerns. Although Saudi Arabia established its eGovernment project in 2005, Saudi government websites have not yet implemented the fundamental best practices for government website design. To encourage more citizens to use available eGovernment services, Saudi Arabia needs to develop a privacy act and enforce the use of standard terminology across all Saudi government websites.

References

[1] CITC. (2007) Internet usage study in KSA - all sectors [online]. Available at: http://www.citc.gov.sa/NR/rdonlyres/2DB93B05-EAFA-4D8F-A680-3AC5CAD2F45A/0/Internet_Usage_Study_in_KSAAll_sectorsEN.pdf.

[2] Sait, S. et al. (2004) 'E-commerce in Saudi Arabia: adoption and perspectives', AJIS, 12 (1), pp. 54-74.

[3] Alharby, M. (2006) Barriers of e-commerce and e-government in Saudi Arabia. Unpublished Master dissertation. Bradford University.

[4] Alotaibi, J. (2006) The e-government in the Kingdom of Saudi Arabia: the perceptions, trust levels and concerns among the Internet users. Unpublished Master dissertation. University of Salford.

[5] Alhazani, N. (2008) E-government services in government agencies. Riyadh: King Fahd National Library.

[6] Cabinet Office. (2004) Guidelines for UK government websites [online]. Available at: http://archive.cabinetoffice.gov.uk/e-government/Resources/handbook/pdf/pdfindex.asp.

[7] Cabinet Office. (2003). Quality Framework for UK Government Website Design: Usability issues for government websites [online]. Available at: http://webarchive.nationalarchives.gov.uk/20081105160428/http://archive.cabinetoffice.gov.uk/e-government/docs/qualityframework/pdf/quality.pdf

[8] Cabinet Office. (2004) Guidelines for UK Government websites: Illustrated handbook for web management teams [online]. Available at: http://archive.cabinetoffice.gov.uk/eGovernment/Resources/handbook/pdf/pdfindex.a sp.

[9] AGIMO. Web guide [online]. Available at: http://webguide.gov.au/#pageBody.

[10] AGIMO. (2004d) Implementing an effective website search facility [online]. Available at: http://www.finance.gov.au/eGovernment/better-practice-and-collaboration/betterpractice- checklists/docs/BPC16.pdf.

[11] Usability.gov. Navigation [online]. Available at: http://www.usability.gov/pdfs/chapter7.pdf.

ISBN: 978-988-14047-2-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

[12] Panopoulou, E. (2008). 'A framework for evaluating web sites of public authorities', Aslib Proceeding: New Information Perspective, 60 (5), pp. 546- 517.
[13] Al-Sobhi, F. Weerakkody V. (2009) The role of information in faciliting e-government diffusion in Saudi Arabia [online] available at: http://www.iseing.org/emcis/EMCIS2010/Proceedings/Accepted%20Refereed%20Pa pers/C97.pdf.
[14] AL-Busaidy, M. Weerakkody, V. (2009) 'E-government diffusion in Oman: a public sector employees' perspective', Transforming Government People: Process and Policy, 3 (4), pp. 375-393.
[15] Lebech, A . (2003) Privacy and e-government: enterprise challenges for Danish government [online]. Available at: http://www.zurich.ibm.com/pdf/privacysummit/Lebech.pdf.
[16] GIPL. (2003) Privacy and e-government: privacy impact assessments and privacy commissioners- two mechanisms for protecting privacy to promote citizen truest Online[online]. Available at: http://www.internetpolicy.net/practices/030501pia.pdf.
[17] Elsheikh, Y. Cullen, A. (2008) 'E-government in Jordan: challenges and opportunities', Transforming Government People, Process and Policy, 2 (2), pp. 83-103.
[18] Lau, E. (2003) Challenges for e-government development. 5th Global Forum on Reinventing Government, [online]. Available at: http://unpan1.un.org/intradoc/groups/public/documents/UN/UNPAN012241.pdf.
[19] Regan , P. (2008). Privacy on an electronic government context. In Chen, H at el. Digital Government: E-government research, case studies, and implementation. Springer Science, Businesses Media, LLC. pp. 127-140.
[20] Taylor Nelson Sofres. (2003) Government online: an international perspective. Annual Global Report [online]. Available at: www.epractice.eu/files/media/media_872.pdf.
[21] AGIMO. (2007a) Australians' use of and satisfaction with e-government services [online]. Available at: http://www.finance.gov.au/Publications/use-of-eGovernmentservices-2007.
[22] Adeshara, P. et al. (2004) 'A survey of acceptance of e-government services in the UK', Journal of Computing and Information Technology,12 (2), pp. 143-150.
[23] Bélanger, F. Carter, L. (2009) 'The impact of the digital divide on e-government use', Communications of the ACM, 52 (4), pp. 132-135.
[24] McMenemy, D. et al. (2007) A handbook of ethical practice: a practical guide to dealing with ethical issues in information and library work. Oxford: Chandos Publishing.
[25] Cullen, R. (2009) 'Culture, identity and information privacy in the age of digital government', Online Information Review, 33 (3), pp. 405-421.
[26] Hussein, A. (2006) 'E-government architecture in Jordan: A Comparative Analysis', Journal of Computer Science, 2 (11), pp. 846-852.
[27] Henari, F. Mahboob, R. (2008) 'E-commerce in Bahrain: the non-technical limitation', Education, Business and Society: Contemporary Middle Eastern Issues, 1 (3), pp. 213-220.
[28] Al-Fawzan, N and Elsayed, O. (2012). Data Protection in the Kingdom of Saudi Arabia: A Primer [online]. Available at: www.lw.com/.../Data-Protection-in-the-Kingdom-of-Saudi-Arabia.

ISBN: 978-988-14047-2-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)