ICIT 2015 The 7th International Conference on Information Technology
doi:10.15849/icit.2015.0066

Privacy Policy of E-Government Websites and the Effect on Users' Privacy

Maryam Al-Jamal & Emad Abu-Shanab
MIS Department, IT College, Yarmouk University, Irbid, Jordan,
maryam.aljamal@yahoo.com & abushanab@yu.edu.jo

***Abstract*—The rapid developments in information and communication technologies require citizens to provide more information to their government within the context of e-government. Providing personal information to e-government websites is necessary to benefit from its services, where providing such information over the Internet raises privacy concerns by users. This paper argues that a privacy policy can be a good guarantee for users' privacy and a factor that supports the intention to use e-government services. The literature and international reports were explored to understand the issues related to privacy policy in e-government and their importance to users. Principle by the OECD and FTC are widely used by researchers to set the stage for better development of privacy policies. Finally, two frameworks were proposed to guide future research and recognize the factors affecting the adoption process of e-government.**

Keywords—E-government, Privacy, Privacy policy, Security, FTC principles, OECD principles, proposed framework.

I.INTRODUCTION

The nature of interaction with information technology requires users to provide more information about them. Internet has the most significant effect on our lives; since we use it for communication, learning, entertainment, business applications and many others. To benefit from all previously mentioned applications, users are required to disclose their private information. Providing such information over the Internet raises many concerns for the users. Privacy of users' information is one of these concerns.

One of the major applications of information and communication technology (ICT) and the Internet is e-government. E-government websites provide us with information and services. The amount of data and information gathered by governments' websites is increasing, and users don't know the extent to which his\her information is secure and protected. The presence of a privacy policy is required in e-government websites to ensure users' privacy.

Although privacy policy can be a guarantee for citizens' data protection on e-government websites, there are still some websites that don't adhere to such provision. Even privacy policy can't be that much effective if there are no privacy protection laws in the country, or no clear definition of privacy policy or what it should contain.

Research indicated that trust in e-government websites is a significant predictor of their adoption of such websites and the intentions to use those [1]. Users' trust in e-government websites can be affected by the presence of privacy policy on their websites. Still there are well crafted privacy policies and deficient ones.

This study will explore the literature to understand the privacy issues related to e-government websites and information systems. Privacy issues revolve around privacy policy, its definition, its importance, and its contents. Also, the factors affecting users' attitudes toward privacy policies will be explored, where we present some globally known principles for developing privacy policies. The presence of privacy policy in e-governments websites will be investigated along with the quality of these policies. The concept of privacy and its implications on e-government is important. Privacy protection solutions will also be presented.

The structure of this paper is as follows: a literature review of previous related work will be presented in an overview of e-government, followed by an exploration of privacy issues in e-government websites. Finally, an investigation of privacy policy in e-government will be conducted to conclude to a conceptual framework to guide our future research. Conclusions and future research will be depicted at the end.

II.LITERATURE REVIEW

Using e-government websites and interacting with its systems and interfaces is the major indicator of such projects success. To enhance the chances of citizens' use of e-government websites, privacy of information should be maintained. The following section will explore the literature related to such issue.

A. Overview of e-government

Many researchers have defined e-government in many several ways. E-government revolves around using the Internet to provide services to citizens, businesses and employees to enhance efficiency and effectiveness of private and public sectors [2]. Others have considered e-government as *"the use of information and communication technology (ICT) and particularly the Internet to deliver information and services by the*

doi:10.15849/icit.2015.0066

government to its customers (businesses and citizens)" [1, p. 39].

In addition to that, e-government is defined as *"the wide and efficient use of application of different technologies by governmental departments and ministries to connect with and better serve the citizens"* [3, p. 278]. For the purpose of this study, and based on the previous definitions explored, we can define e-government as: utilizing ICT tools and applications to provide service and information to citizens, businesses and public employees in a better, more efficient and effective way that protect their privacy of information.

As widely recognized, e-government has many benefits to citizens, businesses and government itself. It's noteworthy to citizens that improving accessibility to public services is important, but enhancing transparency and the effectiveness of government performance is more important. For businesses e-government is suitable, fast and cost-effective for getting the needed information and services. For governments, e-government is an innovative tool that allows governments to know the needs of their people and serve them quickly and at a reduced cost [4].

Generally e-government helps in fighting corruption and bribes [5], reforming the social and economical status in the country, enhancing governance, saving time in providing services and offering the citizens a higher accessibility to policies, standards, laws and information [3]. Also, e-government has been known as an effective tool for increasing accountability, enhancing transparency rates and fostering e-democracy [6] [7].

Besides all previously mentioned benefits of e-government, there are some obstacles and challenges hindering the progress of e-government projects. These challenges may be due to government agencies and their users. Many studies included the following obstacles: privacy issues, digital divide, availability, trust, security application, improper integration between systems and governmental departments, infrastructure costs, lack of legal frameworks supporting e-government and cultural issues [4] [8].

Researchers now view e-government as an effective strategic tool for administrative reform in public sector, at all levels of government bodies. Also, they considered the emergence of web 2.0 tools and development (such as: mobile devices, wikis, blogs and social media) is the reason behind enlarging the spectrum of people participating and interacting with government bodies, and even government agencies among each other. Moreover, government websites can be a great component for facilitating public information sharing [9]. So e-government has many channels to reach its stakeholders besides its websites.

B. Privacy in e-government

Moving from the traditional government to e-government resulted in a loss of privacy and security of users' personal data; this loss was caused by shifting from centralized/closed systems to decentralized/open governance systems. Personal data is defined as any type of data that can reveal person's identity (directly or indirectly). Examples of personal data are: ID number or social security number SSN, employment number, age and religion [10].

Privacy is a broad term that is defined in many ways depending on the context, environment or perspective. However, privacy is the state when an individual can control personal information about his/her self and how, why, what and who knows such information. Other concepts regarding privacy are related to e-government nature; that is "online privacy". Simply, online privacy is person's privacy over the Internet [11].

It is important here to clarify the relationship between privacy and security. It is noticed in the literature that privacy and security are always mentioned together and even explored together within the e-government literature [12]. The reason behind that is that security is known as protecting the system against threats like hackers, crackers and viruses. These risks threat the privacy of systems' users. Then security of the system is the gate to invading privacy of information. So e-government websites need to grant the needed level of privacy along with the security mechanisms intended to be used [13] [14].

The literature of e-business and e-commerce frequently mentioned a situation when the website sells/gives information of users to a third-party, as a threat to privacy. Such situation influences citizens' trust in e-government. Trust in e-government is explored in the literature based on two dimensions: trust in the technology and trust in the government itself [1]. Trust in technology can be solved by enhancing the security levels and the legal framework related to online service. Trust in government is the responsibility of the government itself to improve its image. In the second situation trust is gained in an ongoing process [1].

E-government can bring to societies and public systems more efficiency in offering services, higher accessibility to public services, empowered participation, and better transparency. Public participation is widely recognized for playing an important role in improving government activities and communication with citizens [15]. So information that is provided by citizens through e-government websites should be secured and their privacy must be preserved by the government [4].

As e-government is shifting to open government, more emphasis is put on transparency and information exchange. The more countries are embracing e-government, the more they are enhancing the transparency of their systems [7]. Theoretically speaking, the more transparent organizations are becoming, the more they slip into the trap of violating privacy issues. In some situations organizational transparency is reduced to protect others' rights like privacy [6]. Transparency must be balanced against privacy in a way that adheres with societal norms and without violating international standards.

Research also focused on the adoption process of e-government services where some researchers concluded to a set of factors affecting user's intention to use e-

doi:10.15849/icit.2015.0066

government websites like: system quality, service quality, information quality [16], risk perceptions [12], trust, perceived ease of use, perceived usefulness, and social influence [17]. Others examined several factors that affected the use of SMS based e-government services in Jordan; they found that "perceived risk to users' privacy" has been ranked the fourth among many other factors in predicting the adoption process which indicates the importance of privacy and security [18].

In a study profiling non-users of e-government, it is found that the negative attitude to e-government services was not the reason behind not using the services. Researchers argued that it may be a result of perceived risks (security and privacy risks) in using e-government services. Governments need to pay attention to the importance of high security techniques used in their systems to protect their systems and people's privacy [19]. Such efforts will improve government's reputation and citizens' intention to use its systems.

Users' satisfaction is measured by how frequent they use the service and visit the website again and again. Irani et al. [20] concluded that citizens' satisfaction and trust in e-government are increased when it provides them with secured and privacy oriented systems. So citizens' online privacy must be guaranteed as it is a crucial factor for e-government's success.

A study of citizens' e-government preferences concluded to four segments of users: risk-conscious, balanced, recourse-conservative and usability-focused. The level of privacy that citizens require was affected by the type of service they use. In the same study it is found that citizens' concerns were greater when they filed their taxes online compared to online appointment booking [21].

As mentioned previously, in their pursue to open communication with their citizens and reach them where ever they are, governments utilized social media and tried to benefit from such channel [22]. Using social media channels, many obstacles and threats are facing governments and e-government projects. Examples of these threats are: lack of government possibility to ensure users' privacy, lower control on social media contents, and the absence of legal framework governing activities in social media [23]. It is obvious that the threat level on users' privacy in e-government is related to the channel used by the government.

Regarding privacy protection solutions, there are technical solutions and legal-based solutions. Some researchers asserted that the need for laws to ensure privacy of information is more important. They emphasized the importance of issuing the needed laws and enforcing them. More over e-government has been considered as a tool for pushing forward e-business movement by setting such laws [13].

In an analysis of European Union countries' policies regarding privacy and security; it is found that there is a difference in how each country understands privacy and security issues [24]. The author proclaimed that they shared the assumptions about policy formulation and the need of governmental intervention in the policy formulation process. Such conclusion indicates the difficulty of formulating and issuing the needed laws, standards and policies related to e-government environment.

Many Studies concluded that parties administering e-government projects (mainly the government itself) should develop information security goals and make sure that resources are available to achieve these goals. Surly, an investment in security techniques and mechanisms must be established and developed to improve the security and privacy status. That's because users' privacy concerns play a significant role in affecting e-government performance [14].

C. Privacy policy in e-government

Although users are concerned about their privacy over the Internet they have fair knowledge on how to protect their privacy. Users try to protect their privacy by deleting cookies, being more conservative in providing unnecessary information. There are specialized providers of privacy seals and standards like TRUSTe, PriceWaterhouseCoopers PWC, BBB Online and WebTrust [13]. This study will focus on privacy policy as a major privacy assurance tool.

Privacy policy can be defined as *"legal document that defines how the website gathers information from the user and how it uses this information"* [25, p. 88]. Privacy policy clarifies for website users how their data is being collected, the purpose of data collection, and the different uses of such data. Researchers concluded that culture is a significant factor affecting users' attitudes toward the content of a privacy policy. A group of researchers compared the responses of Russian and Taiwanese users in regard to information provided online; they found that Taiwanese trust has increased when they knew that their information is secured, while Russians trust didn't increase [26].

A study conducted in China found that most websites have a type of privacy discloser. In the same study, it is noticed that the majority of websites collect ID number/SSN; they interpret it as a step by the government to protect their citizens' from fraud. Such step might be considered in other cultures as an intrusion of privacy [27]. Based on the previous two studies, we can infer that the needed privacy level is affected by the difference of cultural perspectives.

Contents of privacy policy mainly depend on laws enforced in the country regarding this issue and the requirements of the organizations interacting with users. Privacy policy should clarify what data is collected from users, why it is collected and how it will be used. Moreover, privacy policy must be readable and understandable by all of the targeted users of the website [28]. The authors conducted a study regarding the Saudi e-government websites, 28% of websites had privacy policy, while the other 72% did show any kind of privacy policy or agreement. On the other hand, among the websites that have privacy policy 60% of them have a well formulated privacy policy and 40% have weak ones. We can infer from the previous study that the

doi:10.15849/icit.2015.0066

presence of privacy policy is not enough, the quality of privacy policy must also be considered.

A proposed framework by Jha and Bose [10] tried to set some set of standards for planning privacy policy; the framework "CCAGM" stands for: centralization, characterization, access gating and monitoring. It is claimed that the framework can be an effective tool for administering security and privacy issues within the e-government context. *Centralization* means storing all data and records in one secure location, and that is intended to prevent duplication and scattering data in locations that might be unsecured. *Characterization* means that data will be classified as private, public or personal. And *Access Gating* is the mechanism of controlling access to data from different users, like password or SSN. *Monitoring* is to monitor various transactions and check standards formed by the central authorities.

Another important issue regarding privacy policies formulation is the frequent changes of privacy policy. A study presented the problem of privacy policy within Facebook context and considered it as a misleading one due to its frequent changing nature. The frequent changes of privacy policies confused the users of the website about what information they are sharing, to whom and how their information is used. Regarding this issue the federal trade commission (FTC) threatened Facebook to take an action against them (as a regulation body), then Facebook reached a settlement to make its privacy policy consistent and transparent [29]. The question of whether government privacy policies are changing frequently emphasizes the importance of governing laws regarding formulating privacy policy.

D. Principles for developing privacy policy

The context, conditions and guidelines for building a privacy policy are researched by non-academic parties, where some institutions consider themselves guardians for the privacy of citizens' data. The Federal Trade Commission (FTC) is one example, and the Organization for Economic Cooperation and Development (OECD) is another example of organizations that have set principles and standards for writing and developing privacy policies. Some researchers considered the FTC principles as more flexible and realistic framework to guide such process [26].

The OECD included eight main privacy principles. These principles are: Safe guard, collection limitation, data quality, purpose specification, use limitation, openness, individual participation and accountability [30]. Safe guard means that data should be protected and secured from any unauthorized access or risks. Collection limitation means that there should be limits for data collection and data should be collected in a legal manner. Data quality means that data should be accurate, up-to-date, complete and relevant to the purpose of collection. Purpose specification reflects the purpose behind collecting the data and must be stated to users (to take their consent) before the collection process starts and whenever the purpose has changed. Use limitation: personal data should not be revealed or used for other purposes than originally intended, unless the user is informed or the law permits. Openness principle means that organizations must make privacy policy explaining their policies regarding data collection and management [31].

Individual participation means that users must have the right to get their data from data collectors, citizens should have open communication with data collectors at any stage, know the reasons behind any denied requests, and to have control over their data (deletion and change). Accountability means that the service provider is responsible for enforcing and adhering to all other OECD principles applied in their system/website [30].

The FTC contains five main privacy principles. These principles are: Notice, choice, access, security and enforcement. Many researchers used these principles in evaluating privacy policies [26] [28]. Notice means that the system/website must explain clearly what data it collects, why and how will be used. Choice: the website should inform users if they will give their data to a third party and why, and must clearly ask for the users' permission. Access: the website should allow users to review, correct or delete personal information collected by the website. Security principle means that any unauthorized access to users' data must be prevented and the highest security mechanisms must be used and applied to protect users' personal data. Enforcement: the website states that there is a law governing any violations of privacy and the website will take actions against the violators according to the stated law [26]. The following table summarizes both OECD and FTC principles, where we matched both set of principles against each other in a proposition for researchers and to guard against redundancy of issues.

Table 1: Matching principles from OECD & FTC

OECD principles	FTC principles	Matched principles
1. Safe guard	A. Notice	(A,4,2)
2. Collection limitation	B. Choice	(B,5)
3. Data quality	C. Access	(C,7, 5)
4. Purpose specification	D. Security	(D,1)
5. Use limitation	E. Enforcement	(E,8,6)
6. Openness		
7. Individual participation		
8. Accountability		

From Table 1 it is noticed that "data quality" principle of OECD didn't match with any principle of FTC principles. That may indicate that OECD principles are more comprehensive than FTC principles. However, Wu, Huang, Yen and Popova [26] used the FTC principles for judging privacy policies because these principles are more flexible and realistic, and they are more oriented to users and risks associated with personal data collection [26, p. 891]. Both OEDC and FTC

doi:10.15849/icit.2015.0066

principles are valid principles and widely recognized ones.

III.PROPOSED RESEARCH FRAMEWORK

As e-government phenomenon is spreading worldwide due to the great contributions of ICT tools, more personal information is exchanged between governments and their citizens. This necessitates posting and enforcing privacy policies on e-government websites. Many studies were conducted on privacy policies in e-commerce websites, and some on e-government websites. To understand the evolving domain of e-government and to understand the factors influencing its success, we have proposed a framework that aligns the directions of citizens with those of the government. The main question is "Does the existence of a privacy policy on e-government website influences users' concerns about their privacy?"

Based on the previous discussion in literature review section, Figure 1 shows a proposed framework for citizens-government relationship regarding privacy. In this framework users and governments are the main players in e-government. When users have the intention to use e-government websites, there are three main important factors that influence their attitudes: security, privacy and trust. On the other hand, governments need to encourage people to use e-government websites (as a measure of success), where they must provide three basic things: enforced laws, privacy policy and security mechanisms. Security leads to more controlled privacy which both facilitates more trust. Corners of the figure represent the most important components: users, government and *privacy dimensions*. Also, in the figure security, laws and trust are supporting components leading to the heart of the relationship "e-government".

The Citizen-Government Privacy Alignment Model (CGPAM) reflects on major issues previously explored in the literature: privacy, security and trust. The technology adoption literature is rich with studies that investigated the perceptional or attitudinal predictors of e-government success. Factors like perceived usefulness, perceived ease of use, social influence, perceived facilitating condition, and many other factors, were all explored in the context of e-government websites. This framework looks from a different angle to the phenomenon, where privacy policy, its contents, and its enforcement perceptions are major predictors of e-government success.

To connect the major stream of research into this framework another framework is proposed which tries to differentiate between the major predictors of use in the literature (perceived usefulness, perceived ease of use and social influence) and what we are concerned about here (security, privacy and trust). We are hypothesizing here that citizens will use e-government websites and services in a shallow mode (simple information, not critical, not financial, and not important) when they feel that security, privacy and trust in jeopardized. While citizens will start an in-depth, real use of e-government services when they feel it is secured, has a privacy policy, and they trust it. Such use will lead to the continuous use, which is the ultimate objective of e-government projects. Figure 2 depicts the Continuous E-government Use Model (CEGUM).

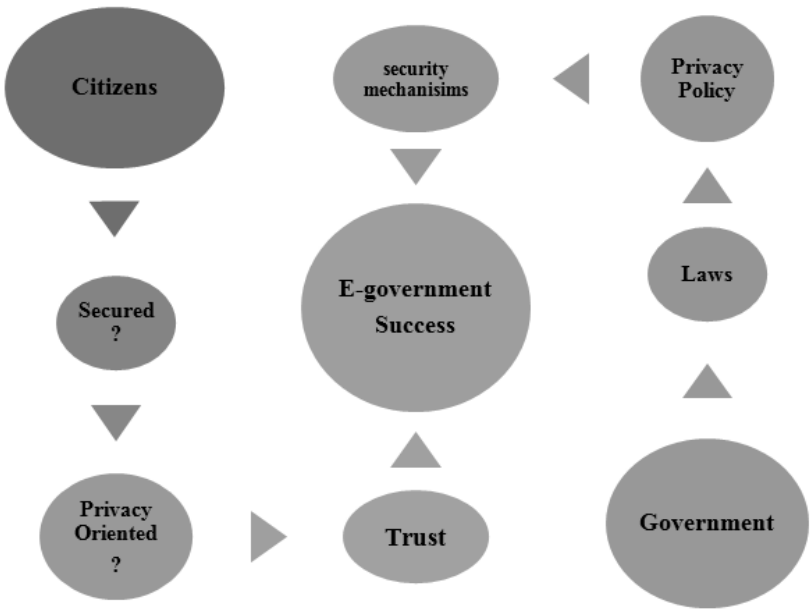

Figure 1: The Citizen-Government Privacy Alignment Model (CGPAM)

doi:10.15849/icit.2015.0066

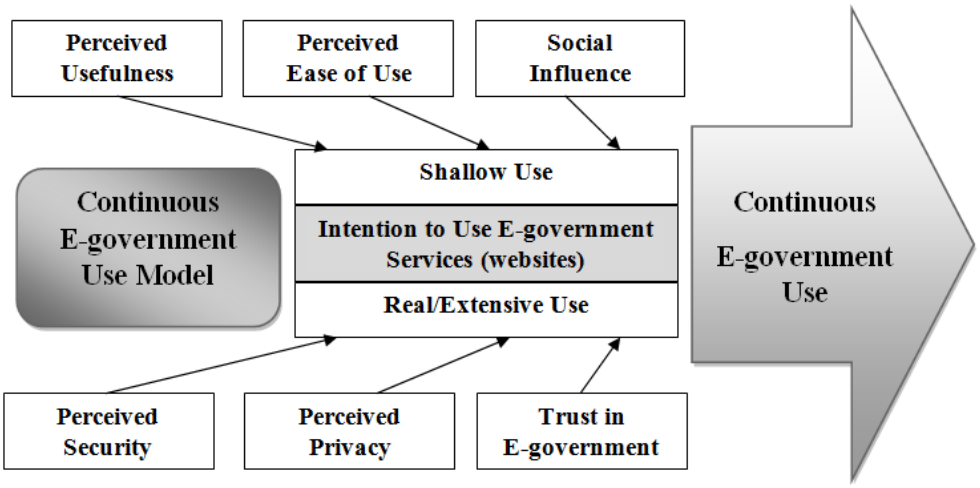

Figure 2: The Continuous E-government Use Model (CEGUM)

IV.CONCLUSION

This paper reviewed the literature to understand the issues related to privacy in e-government and its context. Research and reports asserted the importance of privacy in e-government and its effect on trust and adoption of e-government initiatives among citizens and businesses. Privacy has a significant effect on government performance and users' satisfaction. Privacy level needed is affected by the service being used by the user, and its preservation is achieved by applying high security techniques and enforcing solid laws and regulations. The existence of a privacy policy to aid in defining the relationship between government and users is also significantly important. Privacy policy is a legal document, where users' attitude toward it is affected by their culture. There are many widely known principles for writing privacy policies; the famous ones are visited in this study and they are the FTC and OECD principles.

However, privacy policy existence is not an enough indicator for protecting users' privacy; its quality must also be considered. Also, trust in e-government is a key factor that determines users' beliefs and intentions to use e-government services.

This study proposed two frameworks to guide future research; the first is the Citizen-Government Privacy Alignment Model (CGPAM), which focuses on the alignment between citizens' concerns and government policies and processes. The second framework sums the factors that contribute to continuous use of e-government services/websites. Future research is recommended to test the two frameworks and understand better the context of adopting e-government within a privacy policy context. Also, it is recommended to empirically test the second model to see if such factors are predicting the intention to use e-government and whether it will lead to continuous use.

REFERENCES

[1] Abu-Shanab, E. & Al-Azzam, A. (2012). Trust Dimensions and the Adoption of E-Government in Jordan. International Journal of Information Communication Technologies and Human Development, Vol. 4(1), pp. 39-51.

[2] Nawafleh, S. A., Obiedat, R. F. & Harfoushi, O. K. (2012). E-Government between Developed and Developing Countries. International Journal Of Advanced Corporate Learning, Vol. 5(1), pp. 8-13.

[3] Kayrouz, A. & Atala, I. (2014). E-GOVERNMENT IN LEBANON. European Scientific Journal, Vol. 10(7), pp. 277-283.

[4] Gajendra, S. Xi, B. & Wang, Q. (2012). E-Government: Public Participation and Ethical Issues. Journal Of E-Governance, Vol. 35(4), pp. 195-204.

[5] Abu-Shanab, E., Harb, Y. & Al-Zo'bie, S. (2013). Government as an Anti-Corruption Tool: Citizens Perceptions. International Journal of Electronic Governance, Vol. 6(3), 2013, pp. 232-248.

[6] Halachmi, A. & Greiling, D. (2013). Transparency, E-Government, and Accountability. Public Performance & Management Review,Vol. 36(4), pp. 572-584.

[7] Abu-Shanab, E. (2013). The Relationship between Transparency and E-government: An Empirical Support. IFIP e-government conference 2013 (EGOV 2013), September 16-19, 2013, Koblenz, Germany, pp. 84-91.

[8] Basamh, S. S., Qudaih, H. A. & Suhaimi, M. A. (2014). E-Government Implementation in the Kingdom of Saudi Arabia: An Exploratory Study on Current Practices, Obstacles & Challenges. International Journal of Humanities and Social Science, Vol. 4(2), pp. 296-300.

[9] Sandoval-Almazan, R. & Gil-Garcia, J. R. (2012). Are government internet portals evolving towards more interaction, participation, and collaboration? Revisiting the rhetoric of e-government among municipalities. Government Information Quarterly, Vol. 29, pp. S72-S81.

[10] Jha, A. & Bose, I. (2013). A Framework for Addressing Data Privacy Issues In E-Governance Projects. Journal Of Information Privacy & Security, Vol. 9(3), pp. 18-33.

[11] Brandimarte, L., Acquisti, A. & Loewenstein, G. (2013). Misplaced confidences privacy and the control

doi:10.15849/icit.2015.0066

paradox. Social Psychological and Personality Science, Vol. 4(3), pp. 340-347.

[12] Khasawneh, R., Rabayah, W. & Abu-Shanab, E. (2013). E-Government Acceptance Factors: Trust And Risk. The 6th International Conference on Information Technology (ICIT 2013), 8-10 May, 2013, Amman, Jordan, pp.1-8.

[13] Cepani, L. (2012). The Security and Privacy Issues as One of the Barriers Impeding the E-Business Development in Albania. Annals of the Alexandru Ioan Cuza University-Economics, Vol. 59(1), pp. 353-362.

[14] Zu'bi, M. H. & Al-Onizat, H. H. (2012). E-Government and Security Requirements for Information Systems and Privacy (Performance Linkage). Journal of Management Research, Vol. 4(4), pp. 367-375.

[15] Al-Dalou', R. & Abu-Shanab, E. (2013). E-Participation Levels and Technologies. The 6th International Conference on Information Technology (ICIT 2013), 8-10 May, 2013, Amman, Jordan, pp.1-8.

[16] Qutaishat, F. T. (2013). Users' Perceptions towards Website Quality and Its Effect on Intention to Use E-government Services in Jordan. International Business Research, Vol. 6(1), pp. 97-105.

[17] Abu-Shanab, E. (2014). Antecedents of Trust in E-government Services: An empirical Test in Jordan. Transforming Government: People, Process and Policy, in press and expected to appear in 2014.

[18] Al-ma'aitah, M., Altarawneh, M. & Altarawneh, H. (2012). The state of using SMS-Based e-Government Services: Case Study in Jordan. International Journal of Advanced Networking & Applications, Vol. 4(3), pp. 1591-1600.

[19] Mpinganjira, M. & Mbango, P. (2013). Profiling non-users of e-government services: in quest of e-government promotion strategies. Journal Of Global Business & Technology, Vol. 9(2), pp. 37-46.

[20] Irani, Z., Weerakkody, V., Kamal, M., Hindi, N., Osman, I. H., Anouze, A., & ... Al-Ayoubi, B. (2012). An analysis of methodologies utilised in e-government research A user satisfaction perspective. Journal Of Enterprise Information Management, Vol. 25(3), pp. 298-313.

[21] Venkatesh, V., Chan, F. Y. & Thong, J. L. (2012). Designing e-government services: Key service attributes and citizens' preference structures. Journal Of Operations Management, Vol. 30(1/2), pp. 116-133.

[22] Khasawneh, R. & Abu-Shanab, E. (2013). E-Government and Social Media Sites: The Role and Impact. World Journal of Computer Application and Technology, Vol. 1(1), July 2013, pp. 10-17.

[23] Criado, J. I., Sandoval-Almazan, R. & Gil-Garcia, J. R. (2013). Government innovation through social media. Government Information Quarterly, Vol. 30(4), pp. 319-326.

[24] Barnard-Wills, D. (2013). Security, privacy and surveillance in European policy documents. International Data Privacy Law, Vol. 3(3), pp. 170-180.

[25] Alhomod, S. & Shafi, M. M. (2013). A Study on Implementation of Privacy Policy in Educational Sector Websites in Saudi Arabia. Global Journal of Computer Science and Technology, Vol. 13(1), pp. 22-26.

[26] Wu, K., Huang, S., Yen, D. C. & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. Computers In Human Behavior, Vol. 28(3), pp. 889-897.

[27] Stanaland, A. S. & Lwin, M. O. (2013). ONLINE PRIVACY PRACTICES: ADVANCES IN CHINA. Journal Of International Business Research, Vol. 12(2), pp. 33-46.

[28] Alhomod, S. M. & Shafi, M. M. (2012). Privacy Policy in E Government Websites: A Case Study of Saudi Arabia. Computer & Information Science, Vol. 5(2), pp. 88-93.

[29] Witte, D. S. (2014). Privacy Deleted: Is It Too Late To Protect Our Privacy Online?. Journal Of Internet Law, Vol. 18(1), pp. 1-28.

[30] Allison, D., Capretz, M. A., ElYamany, H. & Wang, S. (2012). Privacy Protection Framework with Defined Policies for Service-Oriented Architecture. Journal of Software Engineering and Applications, Vol. 2012(5), pp. 200-215.

[31] OECD (2013). The OECD website, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data updated in 2013, accessed on April 26,2014: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm