mrp.ase.ro

PRIVACY POLICY OF E-GOVERNMENT WEBSITES: AN ITEMIZED CHECKLIST PROPOSED AND TESTED

[1]Maryam AL-JAMAL and [2]Emad ABU-SHANAB
[1, 2]MIS Dept., IT College, Yarmouk University, Irbid, Jordan
[1]maryam.aljamal@yahoo.com, [2]abushanab@yu.edu.jo

Abstract
Citizens interacting with electronic government websites are keen on the privacy of their information and the security of their data. Providing personal and critical information to e-government websites without any guarantee from the government side to protect such information and use is a risky action. Citizens need to be aware that their information is protected and never misused by their governments. This paper tried to develop a checklist to measure the degree of government websites' adherence to the measures of privacy protection. Publishing a privacy policy can be a first step in guaranteeing users' privacy in addition to other factors needed to reach the required level of protection by international bodies and agencies. The literature and international reports were explored to understand the issues related to privacy policy in e-government and their importance to users. Finally, a test, of a selected set of countries using the specified checklist, was conducted, where results were contrasted to their achievements on the e-government development index.
Keywords: E-government, Privacy, Privacy policy, Security, FTC principles, OECD principles, website test, proposed checklist.

1. INTRODUCTION

Trusting e-government services is crucial and defines the adoption of e-government services. Research indicated that e-government adoption is dependent on many factors like: usefulness, ease of use, trust, security and privacy issues and social influence. The nature of interaction with e-government websites requires citizens to provide more information about them. 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. Providing such information over the Internet raises many concerns for users. Privacy of users' information is one of these concerns. The presence of a privacy policy is required in e-government websites to ensure users' privacy.

Although privacy policy can 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

Management Research and Practice
Volume 7 Issue 3 / 2015
ISSN
2067- 2462

should contain. 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 explored 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 are explored, where we present some globally known principles for developing privacy policies. The presence of privacy policy in e-government websites will be investigated along with the quality of these policies, and some solutions to its issues.

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 empirical test will be conducted to test a proposed checklist that measures the level of adherence to privacy concepts. Conclusions and future research will be depicted at the end.

2. LITERATURE REVIEW

Interacting with e-government websites and its systems is the major indicator of its adoption and success. To enhance the use of e-government websites, privacy of citizens' information should be maintained. The following sections will explore the literature related privacy policy in e-government.

2.1. Overview of e-government

Researchers have defined e-government in many several ways. It is defined as "the use of information and communication technology (ICT) and particularly the Internet to deliver information and services by the government to its customers (businesses and citizens)" (Abu-Shanab & Al-Azzam, 2012, 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" (Kayrouz & Atala, 2014, p. 278). 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 (Nawafleh, Odiedat & Harfoushi, 2012).

This study will adopt the following definition: utilizing ICT tools and applications to provide public service and information to citizens, businesses and public employees in a better, more efficient and effective manner, and adhering to privacy and security guidelines. Such definition takes into consideration the purpose of this study, and the previous e-government definitions cited in the literature.

mrp.ase.ro

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 (Gajendra, Xi & Wang, 2012).

The literature provided empirical evidence that e-government helps in: fighting corruption and bribes (Abu-Shanab, Harb & Al-Zoubi, 2013), reforming the social and economical status in the country, improving the foreign investments attractiveness (Al-Azzam & Abu-Shanab, 2014), enhancing governance, saving time in providing services and offering the citizens a higher accessibility to policies, standards, laws and information (Kayrouz & Atala, 2014). Also, e-government has been known as an effective tool for increasing accountability, enhancing transparency rates and fostering e-democracy (Halachmi & Greiling 2013; Abu-Shanab, 2013).

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 (Gajendra, Xi & Wang, 2012; Basamh, Qudaih & Suhaimi, 2014).

E-government is viewed as an effective strategic tool for administrative reform in public sector, at all levels of government bodies. With all the benefits mentioned previously, many researchers 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. With the massive adoption of social network websites, governments' websites can be a great component for facilitating public information sharing (Sandoval-Almazan & Gil-Garcia, 2012). So e-government has many channels to reach its stakeholders besides its websites.

2.2. 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

Management Research and Practice
Volume 7 Issue 3 / 2015
ISSN
2067- 2462

person's identity (directly or indirectly). Examples of personal data are: ID number or social security number SSN, employment number, age and religion (Jha & Bose, 2013).

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 (Brandimarte, Acquisti & Loewenstein, 2013).

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 (Khasawneh et al., 2013). 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 (Cepani, 2012; Zu'bi & Al-Onizat, 2012).

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 (Abu-Shanab & Al-Azzam, 2012). 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 (Abu-Shanab & Al-Azzam, 2012).

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 (Al-Dalou' & Abu-Shanab, 2013). So information that is provided by citizens through e-government websites should be secured and their privacy must be preserved by the government (Gajendra, Xi & Wang, 2012).

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 (Abu-Shanab, 2013). Theoretically speaking, the more transparent organizations are becoming, the more they slip into the trap of violating privacy issues. In some

mrp.ase.ro

situations organizational transparency is reduced to protect others' rights like privacy (Halachimi & Greiling, 2013). 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-government websites like: system quality, service quality, information quality (Qutaishat, 2013), risk perceptions (Khasawneh et al., 2013), trust, perceived ease of use, perceived usefulness, and social influence (Abu-Shanab, 2014). 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 (Al-ma'aitah et al., 2012).

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 (Mpinganjira & Mbango, 2013). 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. (2012) 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 (Venkatesh, Chan & Thong, 2012).

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 (Khasawneh & Abu-Shanab, 2013). 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

Management Research and Practice
Volume 7 Issue 3 / 2015
ISSN
2067- 2462

framework governing activities in social media (Criado, Sandoval-Almazan & Gil-Garcia, 2013). 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 (Cepani, 2012).

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 (Barnard-Wills, 2013). 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 (Zu'bi & Al-Onizat, 2012).

2.3. 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 (Cepani, 2012). 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" (Alhomod & Shafi, 2012, 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

ISSN 2067- 2462

knew that their information is secured, while Russians trust didn't increase (Wu, Huang, Yen & Popova, 2012).

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 (Stanaland & Lwin, 2013). 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 (Alhomod & Shafi, 2012). 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 presence of privacy policy is not enough, the quality of privacy policy must also be considered.

A proposed framework by Jha and Bose (2013) 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

Management Research and Practice
Volume 7 Issue 3 / 2015
ISSN
2067- 2462

consistent and transparent (Witte, 2014). The question of whether government privacy policies are changing frequently emphasizes the importance of governing laws regarding formulating privacy policy.

2.4. 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 (Wu, Huang, Yen & Popova, 2012).

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 (Allison, Capretz, Yamany & Wang, 2012). 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 (www.oecd.org, 2013).

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 (Allison, Capretz, Yamany & Wang, 2012).

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 (Alhomod & Shafi, 2012; Wu, Huang, Yen & Popova, 2012). 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.

ISSN 2067- 2462

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 (Wu, Huang, Yen & Popova, 2012).

3. RESEARCH METHODOLOGY

This paper tried to understand the issues related to privacy policy in e-government websites. It is evidenced from the literature review that privacy policy is an important factor that increase trust in e-government projects. The major factors that might influence the quality of privacy policy when related to e-government projects can be: human specific, service type and country specific. The human factor is related to people's education, knowledge and the adoption process of e-government services. The type of service is associated to the quality of website and thus indicates a better privacy policy. Finally, the e-government readiness is an indicator of a quality privacy policy.

Based on that, we tried to guide our research by stating the following major questions:

RQ1: How can privacy policy adherence level be measured?

RQ2: What are the factors associated with the quality of privacy policy on e-government websites?

4. DATA ANALYSIS AND DISCUSSION

4.1. A proposed Checklist and Index (PPI)

To answer the first question, a check list was constructed based on the conducted literature review, where the two previously mentioned measures of privacy policy principles were used (OECD & FTC principles). The following table summarizes both OECD and FTC principles, where we matched both set of principles against each other based on their definitions 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		

Management Research and Practice
Volume 7 Issue 3 / 2015
ISSN
2067- 2462

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 (2012) 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 (Wu et al., 2012, p. 891). Both OEDC and FTC principles are valid principles and widely recognized ones.

The next step is to investigate (again from previous literature) the major factors defining a privacy policy index (PPI) of e-government websites. The previous discussion explored two major international measures and concluded to five dimensions that define the degree of website adherence to privacy policy requirements (check Table 1). The following definitions are adopted for the five major measures:

- Notice: Citizens (users) should be notified of any collected data, use or extended use of their information, why information is used.
- Choice: Users are notified if their data will be used by another party, why and how it will be used, and permission is taken for such actions.
- Access: Users have the control over accessing their information, changing it, or deleting it from the system.
- Security: means that data should be protected and secured from any unauthorized access or risks.
- Enforcement: Violations of the previous dimensions need to be controlled and covered by law, where violator's punishment is clearly stated, and the party responsible for such enforcement is stated explicitly.

Based on the five dimensions, a set of items were proposed to measure the degree of privacy policy adherence. The instrument proposed included 14 items and they are listed in Table 2. All dimensions included 3 items except the enforcement dimension, where 2 items were used for evaluating it.

The proposed PPI was pilot tested on 40 countries of the world. The test was conducted on the websites listed in Appendix A, where each item is inspected by the authors and evaluated with a (Yes/No) bases. The value added to the measure if a yes is estimated was 1, where any country can accumulate 14 points if its website adheres to all 14 measures.

Table 2 included in its last column the total countries of the sample used that included the feature. Results indicated that Notice was the best dimension among all five dimensions (65% adherence),

where 26 countries had all three features on their website. The following adherence rank was for two: the first items is # 4 in choice (23 countries), and item # 10 in security (22 countries). The other items were less than 20, which is 50% of countries used.

TABLE 2 - ITEMS OF A PROPOSED PRIVACY POLICY INDEX (PPI)

Dimensions (Items under each dimension)	Total Checked "Yes"
A. Notice *Total item score of dimension (78/120 = 0.650)*	
1. The website explains what data will be collected	26
2. The website clarifies why data will be collected	26
3. The website explains how the collected data will be used	26
B. Choice *Total item score of dimension (50/120 = 0.417)*	
4. The website clarifies if personal information will be disclosed to a third party	23
5. The website explains under what conditions the data will be disclosed	18
6. The website will clearly asks for permission (consent) before disclosing personal information to a third party	9
C. Access *Total item score of dimension (22/120 = 0.183)*	
7. The website allows users to review collected data	10
8. The website allows users to correct (modify) inaccurate collected data	10
9. The website allows users to delete their collected data from the website	2
D. Security *Total item score of dimension (47/120 = 0.392)*	
10. The website clarifies that it takes some steps to provide security for collected data	22
11. The website states that unauthorized access to users' personal data will be prevented	13
12. The website clarifies that it has the advanced technology to protect users' data	12
E. Enforcement *Total item score of dimension (14/80 = 0.175)*	
13. The website states that there is a law governing with punishment those who violate the privacy policy	9
14. The website clarifies that it will take actions according to the law against those who violate the privacy policy	5
F. Total scores (sum of all checked Yes) Privacy Policy Index (PPI) =	Σ

4.2. A pilot test on the PPI

The privacy policy index (PPI) estimated is a measure to the level of privacy policy adherence by countries. It is a numerical measure that can be contrasted to other measures of e-government achievements. To utilize a standard measure for e-government development that is commonly used in reports, we adopted the United Nations e-government statistics published in their 2014 report (UNDESA, 2014). The e-government development index is a composite measure that has three major dimensions: online service index, the human capital index, and the telecommunication infrastructure index.

The second research question, stated previously, implies that certain factors would be associated with this measure. Based on the discussion depicted before the RQs, we can state the following hypotheses:

Management Research and Practice Volume 7 Issue 3 / 2015
ISSN 2067- 2462

H1: The PPI will be positively associated with the e-government readiness index (or development index)

H2: The PPI will be positively associated with the human capital index (in the e-government readiness index (or development index))

H3: The PPI will be positively associated with the online service index (in the e-government readiness index (or development index)).

Appendix A shows the list of countries investigated and the website used. Also, four major columns were added that demonstrate the Privacy Policy Index (PPI) for each country, the E-government Development Index (EGDI), Online Service Index (OSI) and Human Capital Index (HCI). The PPI column is the total sum of "Yes" count for each website on each item listed in Table 2. The last three columns included estimates taken from the country's measure of the "E-government Development Index" reported by the United Nations latest report (UNDESA, 2014).

The last two columns are the previously mentioned indices (the online service index and the human capital index). The reason for such listing is twofold: the first because our argument of the adherence to privacy policy requirements is expected to significantly correlate with how governments are doing in the e-government area. The choice of the EGRI (e-government readiness index) is built around its common use in research and its comprehensiveness with respect to the large number of countries included. The second reason for using the OSI and HCI is the relation of the website structure and how far each country is accomplishing with respect to their website according to the four stage model proposed by the United Nations and the privacy measure. Also, the human capital index provides a foundation for capacity to accept e-government services and watch for privacy policy.

Based on the previous argument, we can check the relationship between the PPI and the three measures (EGDI, OSI & HCI). The relationships between the three e-government indices are expected to yield similar results as they are tautological and the OSI and HCI is part of the EGDI. Correlation results yielded the following matrix shown in Figure 1.

Indicator	PPI	EGDI	OSI	HCI
Privacy Policy Index (PPI)	1			
E-government Development Index (EGDI)	0.838	1		
Online Service Index (OSI)	0.806	0.927	1	
Human Capital Index (HCI)	0.695	0.875	0.659	1

N=40, All correlations are significant at the 0.001 level.

FIGURE 1 - THE CORRELATION MATRIX OF THE 4 INDICES

We can see that the correlations are all significant with a high significance level ($p<0.001$). Such result indicates the high connection between being advanced in e-government and the level of adherence to privacy policy measures. Also, this result supports our proposition of the structure of the proposed PPI. The severely high correlations indicate the high connection between the four measures and open doors for using such index in evaluating websites.

5. CONCLUSIONS

This paper reviewed the literature to understand the issues related to privacy policy 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. This study proposed privacy policy index (PPI) that includes a check list that measures how countries adhere to privacy policy guidelines. The proposed index was pilot tested on 40 countries, where the authors examined their websites and evaluated the proposed 14 items. Results indicated a high adherence with respect to notice dimension (all websites that had a privacy policy, achieved that dimension). On the other hand, some countries accounted for 12/14 items, but others accounted for zero (no privacy policy posted on the site).

Future research is recommended to test the proposed PPI and utilize such important index in evaluating e-government websites. It is obvious that the sample used is a convenient sample with a focus on Arab countries. Future research can examine all countries of the world. Finally, it is important to examine compatible websites with respect to some measure of similarity between them (use the major e-government website of all countries).

REFERENCES

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.

Management Research and Practice
Volume 7 Issue 3 / 2015
ISSN
2067- 2462

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.

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.

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.

Al-Azzam, A. & Abu-Shanab, E. (2014). E-government: The Gate for Attracting Foreign Investments. *The 6th International Conference on Computer Science and Information Technology (CSIT 2014), IEEE conference, Amman, Jordan, 26 & 27-3-2014, pp. 161-165*.

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.

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.

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.

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.

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.

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

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.

Brandimarte, L., Acquisti, A. & Loewenstein, G. (2013). Misplaced confidences privacy and the control paradox. *Social Psychological and Personality Science*, Vol. 4(3), pp. 340-347.

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.

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.

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

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

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.

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.

Kayrouz, A. & Atala, I. (2014). E-Government In Lebanon. *European Scientific Journal*, Vol. 10(7), pp. 277-283.

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.

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.

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.

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.

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

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.

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.

Stanaland, A. S. & Lwin, M. O. (2013). ONLINE Privacy Practices: Advances In China. *Journal Of International Business Research*, Vol. 12(2), pp. 33-46.

UNDESA (2014). United Nations E-Government Survey 2014, E-Government For The Future We Want. A report published by the Department of Economic and Social Affairs, United Nations, 2014.

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.

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.

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.

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.

mrp.ase.ro
Management Research and Practice
Volume 7 Issue 3 / 2015
ISSN
2067- 2462

APPENDIX A: LIST OF TESTED COUNTRIES

			A	B	C	D
	Country	Website	PPI	EGDI	OSI	HCI
1	Korea	www.korea.net	12	0.946	0.976	0.927
2	Australia	www.australia.gov.au/	11	0.910	0.929	0.998
3	Singapore	www.egov.gov.sg/	9	0.908	0.992	0.852
4	USA	www.usa.gov/	9	0.875	0.945	0.939
5	UK	www.gov.uk/help/privacy-policy	7	0.869	0.898	0.857
6	Canada	hwww.canada.gc.ca	9	0.842	0.913	0.895
7	Bahrain	www.bahrain.gov.bh/	10	0.809	0.937	0.784
8	Germany	www.deutschland.de/en	9	0.786	0.669	0.886
9	Italy	www.governo.it/	8	0.759	0.748	0.855
10	Belgium	www.belgium.be/en/	12	0.756	0.677	0.893
11	UAE	www.government.ae/	8	0.714	0.882	0.666
12	Saudi Arabia	www.saudi.gov.sa/	9	0.690	0.772	0.746
13	Qatar	portal.www.gov.qa/	7	0.636	0.654	0.667
14	Kuwait	www.e.gov.kw/	10	0.627	0.575	0.719
15	Oman	www.oman.om/	8	0.627	0.732	0.662
16	Brazil	www2.brasil.gov.br/	7	0.601	0.598	0.737
17	Venezuela	www.gobiernoenlinea.ve/	4	0.556	0.551	0.769
18	Tunisia	www.tunisie.gov.tn/	8	0.539	0.638	0.672
19	Mauritius	www.gov.mu/English/Pages/default.aspx	7	0.534	0.472	0.688
20	Jordan	www.jordan.gov.jo	8	0.517	0.520	0.72
21	Egypt	www.egypt.gov.eg/	8	0.513	0.591	0.591
22	Morocco	www.maroc.ma/	0	0.506	0.693	0.49
23	Brunei Darussalam	www.brunei.gov.bn/en	8	0.504	0.362	0.782
24	Lebanon	www.dawlati.gov.lb/en/disclaimer	7	0.498	0.354	0.737
25	Thailand	www.thaigov.go.th/	0	0.463	0.441	0.664
26	Palau	www.palaugov.net	0	0.442	0.165	0.8
27	Dominica	www.dominica.gov.dm/	6	0.434	0.189	0.67
28	India	india.gov.in/website-policy	5	0.383	0.543	0.47
29	Libya	www.pm.gov.ly	0	0.375	0.016	0.782
30	Ghana	www.ghana.gov.gh/	0	0.374	0.315	0.561
31	Iraq	www.egov.gov.iq/	0	0.314	0.197	0.528
32	Syrian Arab Republic	www.egov.sy/	0	0.313	0.157	0.584
33	Algeria	www.el-mouradia.dz	0	0.311	0.079	0.654
34	Yemen	www.yemen.gov.ye/portal/	5	0.272	0.307	0.384
35	Sudan	www.sudan.gov.sd/index.php/ar/	0	0.261	0.291	0.306
36	Pakistan	www.e-government.gov.pk/	0	0.258	0.323	0.334
37	Mauritania	www.mauritania.mr/	0	0.189	0.047	0.358
38	Comoros	www.beit-salam.km	0	0.181	0.016	0.466
39	Djibouti	www.presidence.dj	0	0.146	0.063	0.318
40	Somalia	www.somaligov.net/	0	0.014	0.016	0