International Journal of Computer and Communication Technology

Volume 8 | Issue 2 Article 7

April 2017

E-GOVERNANCE PRIVACY POLICY, TECHNICAL AND SOCIAL CONCERNS OF PRIVACY IN E-GOVERNANCE FOR INDIA

DR. T. G. K. VASISTA
Vice-Rectorate for Business Development, King Saud University, Riyadh, Saudi Arabia,
gtatapudi@ksu.edu.sa

E-GOVERNANCE PRIVACY POLICY, TECHNICAL AND SOCIAL CONCERNS OF PRIVACY IN E-GOVERNANCE FOR INDIA

DR. T. G. K. VASISTA

Vice-Rectorate for Business Development, King Saud University, Riyadh, Saudi Arabia
E-mail: tgkvasista@gmail.com/gtatapudi@ksu.edu.sa

Abstract- With the introduction of E-Governance, ambient intelligence and ICT applications affect all areas of citizen lives. The field of justice is presenting opportunities and risks that, if mastered now, may offer a route and solution to the dilemma of privacy and scope of encountering it by properly positioning the jurisdiction with better resolutions. Law must be better enforced and more consistently applied across the member states to retain and sustain public credibility, trust and respect by properly safeguarding citizen interests denudes them of government authority especially in a largest democratic country like India. Privacy in cyberspace has been a continuing congressional priority as ICT is becoming pervasive through the implementation of e-governance. There is a need for having privacy law explicitly to India especially within the scope of E-Governance. Discussions are taking place to in the form of proposing it. So this paper while eliciting some of the privacy concerns, suggests that ASCP model can help as an initial level driving index to position the privacy and hence expected to be considered as a prologue to Privacy policy design.

Keywords- *ASCP Model Significance, Data Protection Law, E-Governance, E-Privacy, Privacy Law, Privacy Policy, Right of Privacy, Right of Liberty, IT Law*

I. INTRODUCTION

The emergence of information and communication technology (ICT) has affected the functions and roles of governments in the form of E-Governance implementations. Many governments have realized the benefits of e-governance and have started offering e-services [24]. Privacy in cyberspace has been a continuing congressional priority [8] as ICT is becoming pervasive through the implementation of e-governance. Further it is mentioned in [8] that posting online privacy policies, posting e-mail contact information should be made as e-gov best practices by agencies. In future, there is a possibility that E-Government can adopt new technologies such as grid technology and ubiquitous computing and hence transformation of government will be from e-government to m-government to u-government [14]. But what is proposed is to transform into h-government (helpful government). Helpful government means, it is government that has a real attitude of helping the citizens towards the right direction of in managing their knowledge for their regular e-service needs, protecting their privacy while securing the nation and state from all forms evil both from internal and external to the government and governance.

As commented in [29] that there is deliberate synonymous use of e-government and e-governance terms in literature related to ICT use and applications with government especially while providing quality e-services has been observed. So providing their basic differences can also become helpful in the context of aspiring to design the privacy policy for e-governance. The basic difference in terminology of e-government and e-governance has been addressed by some authors [19] [24] [29] earlier. However the difference of e-government and e-governance are mentioned in [19], based on the focus and centricity, where while e-government focuses mostly on the administration, e-governance on the other hand focuses on the public policy and dissemination and distribution of power. Thus government values possess different nature for privacy concerns measurability. It is argued in [11] that some values of governance such as privacy cannot be defined once for all, as it has no absolute measure. Further it is emphasized in [11] that privacy can be measured only by citizen's preferences.

II. DEFINITION OF PRIVACY

Privacy can be defined as the absence of unreasonable and potentially intrusive collection & use of personal information [14]. The definition of the Privacy is mentioned in [7]. The word privacy has been derived from the Latin word 'Privatus', which mean separate from rest. Further, Privacy can be defined as the "capability of an individual or group secludes themselves or information about themselves and thereby reveal themselves selectively". It is understood as a right of an individual's decision on who can access, what information and when about their personal information [20].

Governments must be responsible custodians for the enormous amounts of personal information and data collected on their citizens through everyday transactions. Protecting the privacy of citizens' personal information stored on these databases is a vital issue while making effective use of the information contained in them [2]. Privacy risk

requires the government to provide assurance on not misusing the citizen's personal data [9] Countries like USA and UK have already introduced their legal framework related to privacy called DPA (Data Protection Act) 1998 and ECPA (Electronic Communications Privacy Act) 1986 respectively. But in India there is no such comprehensive and explicit legal framework that can deal with privacy. However as of now, IT Law is supporting this aspect in association other civil, criminal and business laws in India.

III. RESEARCH STUDY OBJECTIVE

So privacy issue has been becoming the subject of public debates since years. As new technologies are developed, new forms of e-governance applications are emerging and causing increasing raise of privacy concerns. For example, the Grid Technologies, Cloud computing, Web 2.0, wireless based e-services, RFID and EPC networks are some of the examples that are appearing not only in e-governance but also in e-business and e-commerce. Thus, the need for privacy-aware policies, regulations and techniques has been widely recognized by law makers, regulators and the media. As a result, businesses are under pressure to draft privacy policies. Companies are taking pro-active steps to avoid the potential damage of reputation that can be caused by privacy mistakes. So in this connection, new portfolios like chief privacy officer are evolving and making them as essential members of many organisations [13].

Ref. [14] proposed a framework that incorporates the five maturity stages of e-government and their specific requirements from a policy, technology and citizen requirements perspective. In terms of maturity, e-government in India is observed that it has achieved the potential stage of capabilities of using advanced technologies at the information and transaction stage effectively and to some extent in interaction and social networking participation stage but not very effectively in the integration and participation stages. Therefore the objective of this paper is set to explore and elicit the three perspectives of e-privacy concerns mentioned such as policy, technology and citizen requirements above without relating much with the stages of maturity, for discussing the privacy concerns in this paper.

IV. PRIVACY CONCERNS FOR DIGITAL SOCIETY

E-Privacy concerns evolve among the online transactions and risks that influence the use of e-services whether they are related to e-governance, e-business or e-commerce. As mentioned in [14] mentioned that Privacy is more a social concern as against technical concern (e.g. e-security). Identity theft is an example of e-security and privacy breaches that can lead to financial theft, coercion and other privacy risks. Through unreasonable collection and exploitation of personal information, the state could suppress basic human rights and liberties. This in turn can affect the citizen adoption and use of e-government services providing by the government.

A study conducted by [1] in Oman examined the impact of e-privacy risk concerns on the acceptance of e-government services found that e-privacy awareness significantly impacts the level of e-privacy risk concerns. E-Privacy concerns and perceptions of the protection availability against risks can influence citizen's intention to use e-government services. While factors such as Security and Trust-worthiness can help as e-privacy controls so that citizens can confidently use e-services, on the other hand the risk awareness can indirectly reduce the level of trust and in turn reduces the intention to use the services [22] [18], The research study of [1] has used the privacy-trust-behavioral intention model of [17].

Ref. [28] argues that e-privacy protection, although being of interest to many parties such as industry, government and individuals, it is difficult to achieve since the needs and requirements of stakeholders often reflect conflicts and hence understanding e-privacy become an issue

Ref. [4] provides a summarized version of cloud computing privacy concerns, data security issues, laws, regulations and standards in a tabular form. FurtherAbstraction-Standardization-Customization-Personalization (ASCP) model suggested by Ref. [3] has a potential to address the issue of privacy in e-governance. With its classification and depiction as layers, ASCP model can be used to position the scope of privacy. From the scope of privacy perspective, each layer of ASCP from top has a direct relationship to its lower layer. The lower layer contains the upper layer. For example, personalization layer (can be referred to individual privacy) appears within the customization layer (appears as community level privacy). A customization layer appears within Standardization Layer (State level privacy) and so on. It means there is a transitive relationship exists between the personalization layer and standardization layer.

A. Privacy Concerns in USA and Europe

In USA, The privacy act of 1974 protects the privacy of individuals identified in information systems maintained by federal agencies. It is used to regulate the collection, maintenance, use and dissemination of information. It protects the privacy of the citizen by seeking the prior written consent of the individual to disclose the record of personal information. Agencies are mandated to allow the accessibility of individual citizen records whenever interested [8]. Though Freedom of Information Act of 1966 of USA provides

the right of access to federal information to the public, however information pertaining to internal rules, personal issues, trade secrets, individual privacy, items protected by existing laws, information that could affect law enforcement or trials and geographical information on oil wells are exempted. Related to privacy USA has introduced a legal framework called ECPA (Electronic Communications Privacy Act of 1986).

UK has Data Protection Act 1998 that deals with the privacy. Ref. [23] web site mentioned that under the EU's Data Protection Directive, personal data can only be processed under strict conditions. Personal data must be "processed fairly and lawfully" and be collected for "specified, explicitly and legitimate purposes and not further processed in a way incompatible with those purposes". Organisations must then either obtain "unambiguous consent" from individuals before processing is lawful or satisfy one of a number of other conditions. If consent is not obtained, personal data processing can still be lawful providing it is "necessary for the purposes of the legitimate interests" it, or third-parties to who the information is disclosed, is pursuing, providing those interests are not "overridden by the interests for fundamental rights and freedoms of the data subject".

Ref [26] has a good elucidation about privacy and its relationship with the state in USA. He argues that open access to public information and sensitivity to personal activity can, and must be effectively balanced by all levels of government. One key to assuring sufficient protection for personal privacy for governments is to identify a limited range of specific categories of personal information that are so particularly personal and sensitive that they deserve the highest level of protection. Though courts have accepted the assertion that there is a constitutional right to information privacy, but they have clarified that the right is not absolute. Thus, the Privacy act begins from a presumption of personal control over government-held data and vests individuals with the power to waive privacy in such data at their own discretion. Further Raul listed twelve exceptions to federal agency (p. 24) to disclose personally-identifying data without the subject's consent. Most of these exceptions are related to governmental use of personally-identifying data held by a federal agency. Mandated disclosure to comply with the provisions of Freedom of Information Act is one of the privacy Act's most significant exceptions. In Hawaii state personal privacy is an enunciated fundamental right in the constitution. It affirms that the public interest in disclosure must outweigh the privacy interests of the individual.

B. Privacy Concerns in India

In India, the Supreme Court first recognized in 1964 that there is a right of privacy implicit in Article 21 of the constitution, which states that no person shall be deprived of his life or personal liberty except according to procedure established by law. However there is no data protection law in India [15]. The privacy is considered as one of the fundamental rights provided by the constitution. It is interesting to note that Article 21 protects privacy of individual against state only but not against private parties [7] [20]. Privacy issues in the context of third party storage are mentioned in [4].

Ref. [10] presented a legal regime for data protection as a part of NASSCOM initiative. The framework for privacy, data protection and security refers to the following legal aspects of Section 43, Section 65 and importantly Section 72 of IT ACT 2000 which deals with penalty for breach of confidentiality and privacy and Section 66-70: Cyber Security, Section 69: Legal Interception and Monitoring Computer Resource, Section 70: Critical Infrastructure Protection, Section 84A: Encryption of IT (Amendment) Act, 2008 and other laws such as Contracts Acts, Copy Right Act, Banking and Insurance Laws, Telecom Laws, Consumer Laws, Corporate Laws, Intellectual Property Laws of Indian Penal Code and all other acts for e-governance. Creating privacy laws is under discussion stage [15]. Once it is provided, the privacy act may supersede all other privacy clauses which may be present in any other laws of the country [10]. As India is recognized as a business outsourcing leader especially in with its relationship to IT sector, there is an increasing concern about lack of privacy law in India.

1) Privacy Technology for E-Governance: It refers to: Privacy specification language, use of secure multi-party computing techniques, use of electronic security features for preserving privacy in databases, anonymous data analysis, statistical disclosure control, privacy broker for privacy preserving transactions [6][10]. With Open Standards and Free Software, e-government preserves privacy, individual liberties and the right for every citizen to access public information. They are the best technologies to build the citizen trust [9].

2) Privacy Culture in India: From privacy culture perspective, India is somewhat a collectivist society with lower Individualism Index (IDV) and higher Power Distance Index (PDI) as compared to USA, which is an individualist society with higher IDV and lower PDI. Information that might typically be disclosed only to one's spouse or parents in the US is more frequently shared among uncles, aunts and cousins in India [15]. Further the survey conducted by [15] concluded that the concerns and awareness about privacy among Indians is less than that of Americans, Australians, Germans and British people. As Indian outsourcing industry has more concerns about the protection of personal data and new privacy policies, the research results suggests that the awareness of

privacy issues in not sufficient with respect to Indian high tech workforce. Hence the outsourcing industry and international businesses may need to provide privacy training to other workers. Ref [15] concluded that the concerns and awareness about privacy among Indians is less than that of Americans, Australians, Germans and British people. As Indian outsourcing industry has more concerns about the protection of personal data and new privacy policies, the research results suggests that the awareness of privacy issues in not sufficient with respect to Indian high tech workforce. Hence the outsourcing industry and international businesses may need to provide privacy training to other workers.

V. SAMPLE INSTANCES OF ORGANISATIONAL MONITORING POLICY, TECHNICAL AND SOCIAL PRIVACY CONCERNS

Benefits and costs associated with privacy intrusion and protection are complex multi-faced and context specific [5].

For example, the face book policy reports regarding the collection of additional information about its users (through instant messaging). With their policy, it is possible that the person not knowingly provided (for example, the IP address) and the personal data may be shared with third parties [12].

It means in terms of ASCP model, at the personalization level [3], even if personal level specific information is not explicitly specified while using a face book at the community level or making a search at the search engine or at the chat sessions, it is possible to get the observers information through the IP address. Since the ancient times it is considered that IP address and the HTTP cookies is the reliable digital finger print which affects the online privacy and web browser identity [30].

With respect to policy regarding monitoring activities, employees and students in an organization has reported only 46 percent of those individuals with high privacy claimed to have informed themselves about the existence and content of an organizational monitoring policy. From the group of respondents with high privacy concerns 41 percent admitted that they rarely read privacy policies [5]. However, irrespective of whether an individual reads the privacy policy or not, it is important for an organisation to disclose the privacy protection declaration. For example the web site of [31] Identity Theft911 of Scottsdale, Arizona in USA declaration in its policy mentions “Identity Theft911 does not collect personal information from visitors to its website, we do not use cookie’s beacons and do not collect IP Addresses. We do not sell, lease or share information we collect from you with any 3rd parties unless you have provided your consent. (Event then information is only shared for the specific agreed to and identified purposes).”

Further it declares that it makes its best efforts to secure all data on their systems and collected information from individuals using standard industry administrative, technical and operational safeguards. It has to declare the statement like this as a part of U.S/E.U Safe Harbor Compliance [31].

After Yahoo has stopped the facility of chatting against browsing the chat rooms, ‘Telugukadalu.blogspot.in’, one of the regional languages (Telugu) blog, which uploads adult stories and content, has started facilitating the chat session called ‘Nazia Matala Gadhi’ where any user can enter and chat with an anonymous name and gender to chat in Telugu Language. However the IP address will be displayed in the chat session. This site does not verify the age, and does not even provide the warning that the content is strictly for adults, but freely allows to read it by anybody openly. One of the casual persons informed that this site sells this information to prostitutes and adultery brokers to exploit or blackmail the chatter; they do not even hesitate to take the help of some police official in this regard by offering bribe to them [32].

Technically, IP Spoofing [21] though provides privacy by overriding the original identity at the individual level against such exploitations and blackmail scenarios, government may not encourage as it might promote a potential threat to the government monitoring from the security against terrorism activities. IP spoofing is one of the most common forms of camouflage. In IP spoofing, an attacker gains unauthorized access to a computer network by making it appear that a malicious message has come from a trusted machine by ‘spoofing’ the IP address of that machine. In fact, IP Spoofing is punishable in India under section 419, section 465 and section 468 of IT Act [27].

VI. CONCLUSION

Privacy appears to be an important aspect especially while dealing with business and governance aspects. Though human ethics, business ethics and ethical and moral values can provide a kind self-control and self-organizing techniques to limit the risks and affects however, expecting and realizing it within a hugely populated democracy based governance environment does not reflect a realistic situation.

So the overall conclusion is that action is needed now to ensure a balanced and coherent approach to privacy and security in cross-border, inter-agency, intra-agency, inter-institutional and intra-institutional e-sharing information. It is suggested that adding the abstraction levels of ASCP Model proposed by [3] as

a third dimension to the two dimensional Privacy framework proposed by [14] is suggested to be adoptable as a theoretical framework towards finding its effectiveness of applicability and use.

ACKNOWLEDGMENT

I sincerely thank Deanship of Library Affairs, Dr. Mohammed Al-Sudairi of King Saud University for providing Knowledge Resources in this regard.

REFERENCES

[1] Al Abri, D., Tanya,M. and Michael, D., "Examining the Impacts of E-privacy Risk Concerns on Citizen's Intentions to use E-government Services: An Oman Perspective," Journal of Privacy & Security, vol. 5, Iss. 2, 2009. (references)

[2] Almarabeh, T. and AbuAli, A, "A General Framework for E-Government: Definition Maturity Challenges, Opportunities and Success", European Journal of Scientific Research, Vol. 39, No. 1, pp. 29-42, Euro Journals Publishing.

[3] Al Sudairi Mohammed Ahmed Turki and Tatapudi Gopikrishna Vasista, "Achieving Process Standardization in Digital Society with 'ASCP Model", Article ID 759359, Journal of Supply Chain & Customer Relationship Management, Volume 2013 12 pages, 2013.

[4] AlSudairi, M. and Vasista,T. G. K., "Cloud Computing and Privacy Regulations: An Exploratory Study on Issues and Implications", Advanced Computing: An International Journal, Vol.3,No. 2, 2012. pp. 159-169,

[5] Acquisti, A., & Grossklags, J., "Privacy and rationality in individual decision making". Security & Privacy, IEEE, 3(1), 2005, pp. 26-33, 2005.

[6] Bhattacharya, J., "Privacy Middleware for Preserving Privacy in Databases: A Pioneering Privacy Preserving Middleware Concept", VDM Publishing, 2009.

[7] Chaurasia, Ardhapurkar, Srivastava and Sharma (Undated), "E-Privacy and Data Protection in Indian Perspective: Legal Technical and Political Challenges, Proposed Framework",[Online] https://lawlib.wlu.edu/lexopus/works/547-1.pdf, (Accessed on March 14, 2013).

[8] Garson, G. D. Public Information Technology and E-Governance: Managing the Virtual State, Jones and Bartlett Publishers Inc, 2006

[9] Georgescu, M. "The Government in the Digital Age: Myths, Realities and Promises. Innovative Applications of Information Technologies in Business and Management", Forthcoming. Available at SSRN: http://ssrn.com/abstract=906587, 2008.

[10] Godse, V. "Data Security in E-Governance Projects in India". Proc. of RISE Conference, Brussels, December 9, 2010

[11] Gronlund, A., "The Years of E-Government: The 'End of History' and New Beginning". In M.A. Wimmer et al. (Eds.) EGov IFIP International Federation for Information Processing, LNCS 6228, 2010, pp. 13-24.

[12] Gross, R. and Acquisti, A., "Information Revelations and Privacy in Online Social Networks (The Facebook case)", Pre-Proceedings version for ACM workshop on Privacy in the Electronic Society, WPES-2005.

[13] IBM-ZURICH, "E-Privacy – Privacy in the Electronic Society",[Online] http://www.zurich.ibm.com/~gka/ePrivacy/ (Accessed on March 14, 2013)

[14] Kumaraguru, P. and Cranor, L. "Privacy in India: Attitudes and Awareness", 2005 [Online] http://www-cgi.cs.cmu.edu/afs/cs.cmu.edu/Web/People/ponguru/PET_2005.pdf

(Accessed on March 13, 2013).

[15] Litman, J. "Information Privacy/Information Property, Stanford Law Review", Vol. 52, 2000, pp. 1283-1312, [Online] http://www.asc.upenn.edu/usr/ogandy/c734%20resources/litman%20privacy-property.pdf (Accessed on March 14, 2013).

[16] Liu,C., Marchewka, J., Lu, J., and Yu, C. S. "Beyond concern a privacy-trust-behavioral intention model of electronic commerce", Information & Management, 42(2), 2005, pp.289-304.

[17] Lodge, J. and Robinson, A., "JFS and Judicial Cooperation: Quality and Ethics for eGovernance", 2005, [Online] http://danskprivacynet.files.wordpress.com/2008/06/5-quality_ethics_egovernance_en.pdf (Accessed on March 14, 2013)

[18] Malhotra, N. K., Kim, S. S. and Agarwal, J. "Internet users information privacy concerns: the construct, the scale and a casual model", Information Systems Research, 15(4),2004, pp. 336-355.

[19] Marche, S. and McNiven, J. D,"E‐Government and E‐Governance: The Future Isn't What It Used To Be." Canadian Journal of Administrative Sciences/Revue Canadienne des Sciences de l'Administration 20.1 (2003): 74-86.

[20] Mather, T., "E Privacy and Data Protection in Indian Perspective. Nation", [Online] https://lawlib.wlu.edu/lexopus/works/547-1.pdf (Accessed on March 14, 2013)

[21] Milne, G.R., Rohm, A.J. and Bahl, S. "Consumers' protection of online privacy and identity, Journal of Consumer Affairs", Vol. 38 Iss. 2, 2004, pp.217-232, Wiley Online Library.

[22] Olivero, N., and Lunt, P., Privacy versus willingness to disclose in e-commerce exchanges: the effect of risk awareness on the relative role of trust and control. Journal of Economic Psychology, 25(2), 2004. pp. 243-262.

[23] Out-law.com, "Discrimination between public and private personal data contrary to balanced rights, ECJ rules", November 2011 [Online] http://www.out-law.com/en/articles/2011/november/discrimination-between-public-and-private-personal-data-contrary-to-balanced-rights-ecj-rules-/ (Accessed on March 13, 2013)

[24] Palanisamy, R. "Issues and Challenges in e-governance planning", Electronic Government an International Journal, Vol. 1, No. 3, (2004), Inderscience Publishers.

[25] Palvia, S. C. J and Sharma, S. S., "E-Government and E-Governance: Definitions/Domains Framework and Status around the world", 2007, [Online] http://www.iceg.net/2007/books/1/1_369.pdf (Accessed on March 13, 2013)

[26] Kessler, K, Hettich, N, Parsons, C., Richardson & Triana, A. "A framework for Assessing Privacy Readiness of e-Government", Manchester Centre for Development Informatics, iGovernment Working Paper 21, IDPM, University of Manchester, UK, 2011.

[27] Roul, A. C., Privacy and the Digital State: Balancing Public Information and Personal Privacy, 2002, Kluwer Academic Publisher.

[28] Shahu, R. "IP Spoofing" [Online] http://share.pdfonline.com/d0ba29e540294c088d3f4ff11a779d2a/3.%20report.htm, (Accessed on June 7, 2013)

[29] Shata, O., "E-Services Privacy: Needs, Approaches, Challenges, Models and Dimensions". In I. Lee (Ed.), Electronic Business: Concepts, Methodologies, Tools, and Applications, Hershey, P.A. Information Science References, 2009, pp. 2099-2114, doi:10-4018/978-1-60566-056-1.ch130.

[30] Tatapudi, G. V. and AlSudairi, M. A. T. (2013), Suggesting Service Quality Model for E-Governance, ECEG13, July 13-14, Como, Italy,

[31] http://www.browserleaks.com/ [Online] (Accessed on June 7, 2013)

[32] http://www.idt911.com/en/PrivacyPolicy.aspx [Online] (Accessed on June 7, 2013)

[33] http://telugukadalu.blogspot.in/ [Online] (Accessed on June 7, 2013)