A Strategic Insight into Electronic Government, Data Collection and Privacy Issues in India

Ranjan Chaudhuri[1]

ABSTRACT

The integration of electronic governance and protecting privacy interests and the subsequent implementation to enhance service efficiency and ease of use for citizens is not simple. The technologies that make the World Wide Web and e-government possible have some potentially negative aspects. Privacy issues are a major concern for many, since there are the means to collect consumer information easily with digital tools. Transaction security is equally important as well. These issues need timely resolution with government and business working together to ensure the privacy of consumers and the fidelity of transactions. Business and government need to develop a set of specific standards that are part of a uniform business code for transacting business on the Internet. The governments, both at the central and the state level have realized the benefits of e-governance and have started offering their services through the internet. Based on a review of literature, this paper summarizes the recent privacy and security issues from a strategic perspective and challenges in e-governance development.

Keywords: e-governance, information and communication technology, strategy, trust, privacy, security

1. Introduction

E-governance in India has been a focus area recently. Some of the success stories have also been publicized. Information and Communication Technology (ICT), especially Internet, being a powerful tool, provides immense potential for the government to improve its servicing of the citizens. The governments, both at the center and at the states, in India have taken the e-governance seriously and have been continuously endeavoring to provide citizen services in a better manner. There have been several successful initiatives and many noteworthy case studies have been prepared on these. The M S Swaminathan Research Foundation Rural Tele-Centers in Southern India has been very successful by adopting participatory service delivery methods (Sarker, 2003). Some of the other successful initiatives are Gyandoot, e-seva, Bhoomi and CARD. Several projects in diverse places such as in the slums of New Delhi, in the fishermen's' communities of Pondicherry and in the villages of Madhya Pradesh, have demonstrated the efficacy of IT in enlivening the living by improving the means of livelihood for the people on the other side of digital divide (poor and semi-literate people) who are normally excluded from such projects (Sood 2004). While the initiatives of the governments (both center and state) in India in the field of e-governance have been praiseworthy, continuing and augmenting them is a major concern. With properly structured process and workflow parameters, the delivery mechanism and access facilities should be designed to provide smooth and hassle-free service delivery to the citizens. Use of ICT as the enabler can help in this as well as in

[1] National Institut of Industriel Engineering (NITIE), Mumbai, India (Email: ranjan@nitie.edu, Telephone: Mobile: +91-9969107510)

ensuring the security of data and privacy issues. The present projects in India are very weak in these aspects. Some of the examples of technology enablers are records (data) management system, Internet, broadband, touch-screen kiosks, and etc. Digital information can be highly risky. Data can be intercepted by organizations or individuals that will sell it to other parties, alter it, or use it for a variety of purposes. The need for fast and reliable information exchange between citizens and the government has certainly fueled the growth of the electronic governance so far. If the integrity and confidentiality of information cannot be protected, then the potential of electronic governance would be minimized to a considerable extent. This article provides a framework for understanding the implications of privacy and security in the public domain, the challenges for increasing use of the Internet to deliver services and information, and the connections and lessons that can be learned from the best practices with privacy and security issues. Privacy and security practices in e–commerce can provide input into the issues of public use of the Internet for e-government.

2. Strategic Issues for E-Governance: Privacy, Authentication and Security

The privacy of the citizen also needs to be ensured while implementing e – governance in the country. Whenever a citizen gets into any transaction with a Government agency, he keys in lot of personal information, which can be misused by the others. Thus, the citizen should be ensured that the information flow would pass through reliable channels and seamless network (Gartner, 2000). Secured ways of transactions for the Government services are another issue of concern. The identity of citizens requesting services needs to be verified before they access or use the services. Here digital signature will play an important role in delivery of such services. But the infrastructure needed to support them is very expensive and requires constant maintenance. Hence a pertinent need still survives, compelling the authorities to ensure the authenticity in their transactions thereby gaining absolute trust and confidence of the citizen. While the benefits to be gained are immense, the potential pitfalls are just as large (Gartner, 2000). The security of e-governance decreases as its functionality requires the use of distributed applications that execute many transactions against multiple databases. Given the potential for abuse, it is only a matter of time before legislation will mandate privacy and security mechanisms. There is some evidence to indicate Internet community will welcome government intervention on this matter. In a *Business Week* survey (Green, Yang, and Judge 1998), the majority cited privacy concerns as the number one reason they are not using the web based transactions.

Collection of data about individuals has always invoked issues of privacy. However, online technology increases the concerns as it allows for storage of more data, faster and easier than before. In addition, it allows for easier manipulation of that data and cross-referencing at unbelievable speed (Punch, 2000). Finally, in the online world, data collection can also occur without the knowledge of the individual. Traditional limitations on the power of government to intrude into citizens' lives begin with the Indian Constitution. The power of the government and law enforcement has been clearly defined. It is important to note the existence of these protections as part of the underlying and fundamental policy of constraining government actions and protecting citizen privacy under the rights guaranteed by the Indian Constitution. Further Indian citizens have the right to seek information under the Right to Information Act.

3. Consumer Privacy Concerns in E-Government

Unlike in electronic commerce, there have been no detailed studies of consumer perceptions of the privacy and security of C2G transactions at government websites. This is an area that should be studied, taking into consideration the relationships and the structure of e-governance in the country. One of the most sensitive areas of Indian consumer's perception of personal information is the Permanent Account Number (PAN). Access to an individual's PAN can facilitate the collection of additional information and can lead to personal financial information theft. Same concern is there for divulging credit card information or bank account information on the web.

Besides the issue of cross-referencing data between online and offline databases, collection of data without consent is the biggest issue privacy advocates are raising with online websites. As users customize their web browsers with personal information, they do not always realize that this information can be accessed from websites they are visiting and then stored in the website's databases. Usually this is accomplished by means of "cookies."

4. Recommendations

The issue of privacy for electronic government is a complex one that requires a thorough investigation of the implications for all constituents. There are some recommendations that can be made (Janine, 2001). This section presents some of the major recommendations applicable in India.

- The government must meet the country's legal and constitutional requirements to instill confidence and trust in government.
- Make electronically available information in an easy to read, consumer – friendly and understandable format.
- Consider the collection of IP addresses as "personally identifiable information" under the Privacy Act.
- Create a government privacy seal program and develop standard, precise, and clear privacy statements. The central government must work with state and local governments and agencies to develop standardization and shared privacy standards.
- Educate constituents on privacy and security in e-government.
- The government must gain the confidence and trust of businesses by encouraging participation in the marketplace and creating efficiencies.

5. Building Legislative Infrastructure for e-governance in India for protecting privacy issues

E-Governance requires a range of legislative changes including electronic signatures; electronic archiving; data matching; freedom of information; data protection; computer crime; and intellectual property rights legislation. Regulatory changes are required for a host of activities from procurement to service delivery. All changes would typically form part of broader change to support generic e-economy and e-nation initiatives. The Government of India has already introduced the IT Act and Convergence Bill.

The following needs to be done to protect citizen and consumer security and privacy in above direction:

- Law for Privacy: will ensure that the information about the Citizens is not misused.
- Prudent application of Right to Information (RTI) Act allowing access to citizen to Government data.
- Amendments to Consumer Protection Law, Tariffs and Taxation Laws, Intellectual Property Regulations etc are required.
- Further guidelines for Content, Technological Standards, and Electronic payments are also necessary.

6. Concluding Remarks

The issue of trust in e-governance is fundamental to its eventual success. If consumers cannot trust that personal information is safe and secure, the e - governance will never reach its potential. Guidelines like those outlined by above, in conjunction with independent auditing, are a start. Government agencies, in conjunction with the industry, should consider establishing an "E - Governance Citizen's Bill of Rights." This bill would categorically outline the legal policies that Web sites must follow and the remedies for redress available to consumers or citizens to the sites who have suffered harm. There should be substantial penalties for those sites and their administrators who fail to address. Government and citizens must work together on encryption, resolving not only the power of the tools themselves but government access to keys

necessary to decipher encrypted information. By working together with government agencies, citizens and consumer forums can influence the type of safeguards that are put into practice. If there is resistance to cooperation with government agencies and the incident of fraud, crime and privacy continues to rise, legislative and other political solutions will be potentially more rigid (Nash, 1997). The electronic governance in India offers enormous potential but measures need to be developed to prevent abuses from occurring in this environment. These issues need swift resolution now in a cooperative climate of consumer and government working together.

References

1. Sarker P.P. (2003), Government Technology International - Sustainability of South Asian ICT Initiatives, *Center for Digital Government*; www.centerdigitalgov.com
2. Sood A.D. (2004), Background & Perspective, *InfoChange, India*; www.infochangeindia.org
3. Gartner Group, E-Government Security: Voting on the Internet, *Research Notes, Strategic Planning Assumption*, January 18, 2000.
4. Gartner Group, E-Government Strategy: Cubing the Circle, *Research Notes, Strategic Planning Assumption*, April 20, 2000.
5. Gartner Group, Key Issues in E-Government Strategy and Management, *Research Notes, Key Issues*, May 23, 2000.
6. H. Green, C. Yang, and P. C. Judge, (1998), The Internet: A Little Privacy, Please, *Business Week* (March 16)
7. Punch, L., (2000) Big Brother Goes On-Line, *Credit Card Management*, (13:3), June 2000, pp. 22-32.
8. Janine S. Hiller, (2001) France Bélanger, Privacy Strategies for Electronic Government, The PricewaterhouseCoopers Report on the The Business of Government, 2001
9. White Paper on E-Governance Strategy in India, Sameer Sachdeva, December 2002
10. M. Nash, (1997), Future of Web Success Relies On Converging Micro-Payment Model with Privacy Technology, *Gartners Group Leaders Online*

About the Author

Ranjan Chaudhuri is an Assistant Professor in Marketing at National Institute of Industrial Engineering, Mumbai. Dr. Chaudhuri's current teaching and research interests are in the area of Retail Management. He has presented papers in International Symposiums in Japan and Russia. He is the recipient of Jawaharlal Nehru Memorial Award, 2001 for best paper in the Journal of the Institution of Engineers' (India), Interdisciplinary Division. Dr Chaudhuri is in the Reviewer's Board of International Journal of AMSE, France. Dr Chaudhuri authored/coauthored more than 30 publications in referred National and International Journals and Conference Proceedings and contributed chapters in three books.