Social Networking, **2013, 2, 47-56**
http://dx.doi.org/10.4236/sn.2013.22006 Published Online April 2013 (http://www.scirp.org/journal/sn)

Social Media in e-Governance: A Study with Special Reference to India

Mohamad Tariq Banday[1], Muzamil M. Mattoo[2]
[1]Department of Electronics & Instrumentation Technology, University of Kashmir, Srinagar, India
[2]University Administration, University of Kashmir, Srinagar, India
Email: sgrmtb@yahoo.com, muzamilmasood@gmail.com

Received February 8, 2013; revised March 11, 2013; accepted April 3, 2013

ABSTRACT

This paper makes an attempt to analyze current use of social media and their promising advantages for e-governance in government organizations. It discusses potential issues especially issues related to security and privacy of individuals, employees, infrastructure and data that impede successful implementation of social media for e-governance. It examines draft government of India framework for embedding social media in organizational structure and examines issued guidelines for platform to be used, authorization to engage on behalf of government organization, scope and extend of such engagement, etc. It compares these guidelines with similar guidelines of some other nations in terms of employee's access, account management, acceptable use, employee conduct, content, security, legal issues and citizen conduct and enumerates its merits, demerits and scope for further improvements.

Keywords: e-Governance; Social Media; Social Media Policy; Social Media Framework

1. Introduction

Social media provides users with deep and rich experience for participation, interaction and collaboration. Various social media tools allow their users to create and share information on the web and collaborate with others interactively thus making easier to find information and connect online with one another. Social media has also been used for e-learning as they have created opportunities for effective teacher-learner, learner-learner and teacher-teacher communication, interaction and collaboration. With the inclusion of mobile technology, there has not only been an intense rise in the number and type of social media tools but their use is also on increase. In developed countries like USA, Poland, UK and Korea at least four in ten adult citizens use social media tools. Social media sites dominate the Internet usage in Asia and the Pacific [1]. In comparison to men, women are more actively engaged in social media sites [2]. Though currently the use of social media sites is more popular among youngsters but studies are revealing that there is an increasing trend of participation by elders from last few years. In general social media can be classified in the following four categories: 1) online networks and ecosystems—e.g. Facebook LinkedIn, MySpace and Twitter, 2) online publications—e.g. YouTube, Flicker, RSS, SlideShare and Twitter, 3) Online collaborative platforms—e.g. Wikis like MediaWiki, blogs like Wordpress or Blogger, and collaborative office solutions like Office-365, Google Docs, MS Lync, Debategraph, Teamwork or WorkSpot, and 4) online feedback systems—e.g. voting and debating, rating and commenting, surveys, polls, blogs, etc. Online networks and ecosystems build and reflect the networks and relationships between peers. Online publication tools provide services or platforms for sharing and publishing content online. Collaborative platforms facilitate cooperative and work processes between people. Tools for online feedback facilitate input from an audience through one-way or two-way communication. To promote business many organizations have included social media in their organizational structure. Governments of various nations have also incorporated social media in e-governance, however, to make this integration secure and more efficient they have devised frameworks, policies and guidelines that regulate this integration.

The remaining paper is organized as follows: Section 2 briefly presents current use of social media in e-governance, followed by discussions on its potential advantages and involved risks in Sections 3 and 4 respectively. Section 5 presents the highlights of a recent study that analyzed 26 social media documents. In Section 6, core elements of a successful social media policy are enumerated. In Section 7, Indian Government framework & guidelines for use of social media in e-governance are examined and its limitations are enumerated in Section 8. Finally, Section 9 provides guidelines for improving this framework followed by conclusion.

2. Social Media in e-Governance

Commercial organizations, academic institutions and individuals use social media extensively for online presence, promotion of goods and services, gathering customer feedbacks, experience sharing, consumer and customer interactions, collaborative content preparation, e-learning, communication, social interaction, etc. Recently, politicians, citizens, and governments throughout the globe including those from least developed countries have demonstrated effective use of social media tools to revolutionize governance arrangements, mobilize movements against and in support of governments, hold election campaigns, sustain government-citizen communication in disorder, etc. Barack Obama and Mitt Romney have actively embraced Twitter and used the social networking sites as campaign tools during the 2012 presidential contest to communicate directly with supporters and, more importantly, drive the political conversation in a way that reaches far beyond the site. Governments under some policy or government officials in their personal capacity have been using social networks for foreign affairs, administration and information. USA and UK governments beside others like Australia and Sweden are most active in the use of social media for digital diplomacy. Currently, 66 percent of all USA Government agencies use one or the other form of social media website [1]. According to the UN e-Governance survey 2012 [3], 48 percent *i.e.* 78 member states provide either a “follow us on Facebook” or “follow us on Twitter” statement on their government websites. According to same survey 7 percent such websites provide chat rooms or IM features to gather public opinion. In India, various ministers and officials actively use social media to communicate with citizens.

Recently, Prime Minister Manmohan Singh has also shown his presence on Twitter as his office launched its social media initiative through Twitter (http://twitter.com/#!/pmoindia), You Tube (http://www.facebook.com/pages/Indian-Prime-Ministers-Office/107934225905981) and Facebook (http://www.youtube.com/user/zPMOffice India?ob=0&feature=results_main). Similar efforts have been initiated by various other ministries and other government functionaries throughout the country.

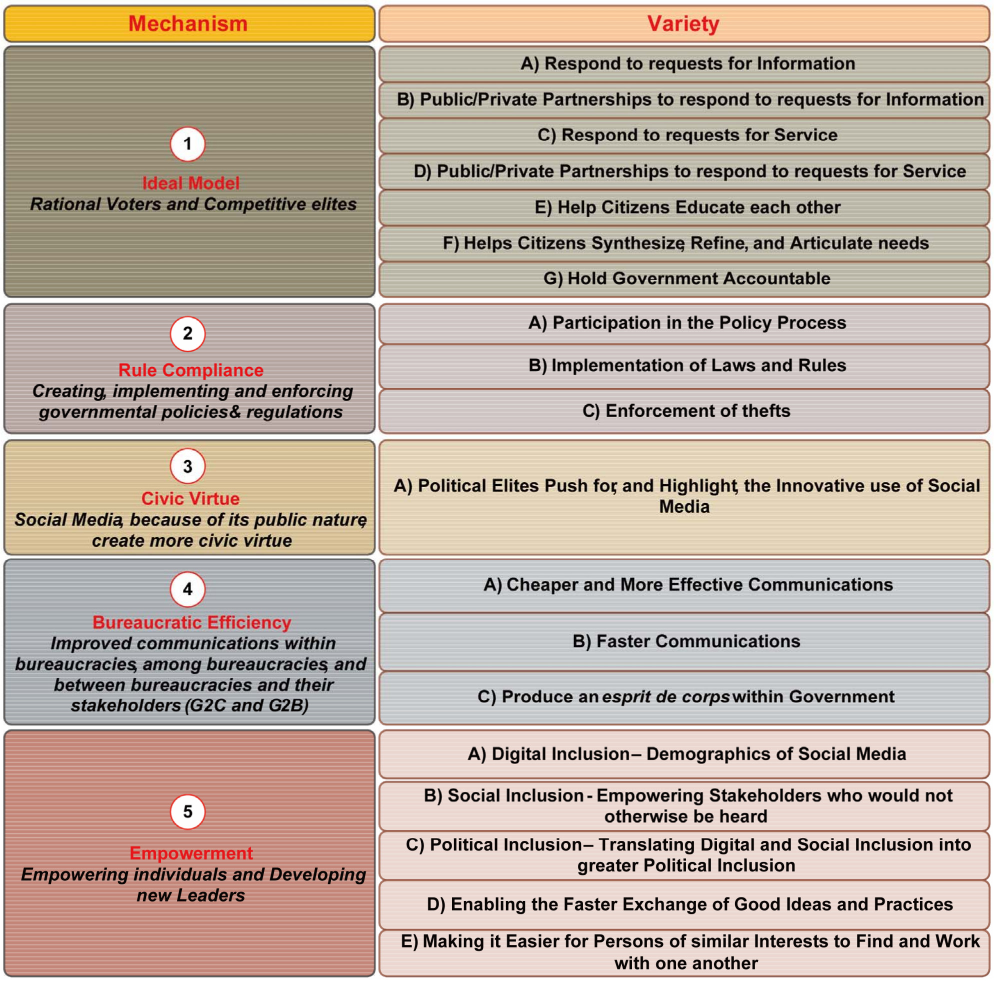
3. Advantages of Using Social Media in e-Governance

Various impediments for adoption of e-governance include lack of awareness of e-services [4], access to e-services [5-6], citizens interest [7], government support [8], digital divide [9] and low usability of government websites. Another important factor in adoption of new technologies required in e-governance is trust on government. Communication with citizens has been recognized as the most important measure to build this trust towards e-governance [10-13].

The four major potential strengths of social media sites are collaboration, participation, empowerment, and time. These facilitate governments to serve its people as they promote government information, services and collaboration with its stakeholders bringing together government agencies, citizens, agencies work and information. Social media can expand the usage of Internet to realize the full benefits of e-governance. Social media sites not only offer benefits to e-governance by intensifying and monitoring services but also reduce costs while improving their quality. Using these sites, governments can post job advertisements, promote services, announce and market events, seek public feedbacks and cooperation and collaborate across its geographically diverse agencies. Since social media has enormous prospectus for increasing citizen usage of e-service [14] and e-participation [15], its greater usage by public could increase transparency which in turn can increases trust on government. A recent review [16] of social media use in e-government has listed its various other applications in e-governance. In its recent report captioned as “Designing Social Media Policy for Government: Eight Essential Elements” [17] three different ways of use of social media sites by employees at work have been identified by Centre for Technology in Government, University at Albany. These uses are for official agency interests, professional interests, and personal interests. Often these three are not mutually exclusive and sometimes there are no clear lines dividing official agency use from professional use or professional use from personal use. David Landsbergen in his recent research works [18,19] identified ways in which social media tools are used in different government agencies and collected five mechanisms as shown in **Figure 1** by which social media tools can realize Government 2.0.

4. Risks in the Use of Social Media for e-Governance

Government information systems including its infrastructure, individuals, agency, employees and information is facing threats that are persistent, pervasive and aggressive [20]. This situation gets intensified by the



Mechanism	Variety
1 Ideal Model *Rational Voters and Competitive elites*	A) Respond to requests for Information
	B) Public/Private Partnerships to respond to requests for Information
	C) Respond to requests for Service
	D) Public/Private Partnerships to respond to requests for Service
	E) Help Citizens Educate each other
	F) Helps Citizens Synthesize, Refine, and Articulate needs
	G) Hold Government Accountable
2 Rule Compliance *Creating, implementing and enforcing governmental policies& regulations*	A) Participation in the Policy Process
	B) Implementation of Laws and Rules
	C) Enforcement of thefts
3 Civic Virtue *Social Media, because of its public nature, create more civic virtue*	A) Political Elites Push for, and Highlight, the Innovative use of Social Media
4 Bureaucratic Efficiency *Improved communications within bureaucracies, among bureaucracies, and between bureaucracies and their stakeholders (G2C and G2B)*	A) Cheaper and More Effective Communications
	B) Faster Communications
	C) Produce an *esprit de corps* within Government
5 Empowerment *Empowering individuals and Developing new Leaders*	A) Digital Inclusion– Demographics of Social Media
	B) Social Inclusion - Empowering Stakeholders who would not otherwise be heard
	C) Political Inclusion– Translating Digital and Social Inclusion into greater Political Inclusion
	D) Enabling the Faster Exchange of Good Ideas and Practices
	E) Making it Easier for Persons of similar Interests to Find and Work with one another

Figure 1. Mechanisms by which social media tools can realize Government 2.0.

environment created by social media because it uses Web 2.0 technologies that are constantly changing and involves risks on multiple fronts including those related to behavior, ergonomic configuration, regulation and technology [21]. Since the risks involved are interdependent, therefore, regulating one may intensify the other.

Since the Web 2.0 environment provides its users with immense power to collaborate, share and interact, they can easily indulge in practices that could infringe the rights of others. The most common risks related to behavior of users during interactions on the Web are risks to reputation, privacy, intellectual property, and publication of personal and illegal content. Social media has potential to raise campaigns in favor or against governments or groups. There has been a sinister use of social networking tools as well, e.g. during summer 2011 riots in the UK. In Kashmir, 2011 upsurge of separatist movement causing unrest in the Kashmir was also directly influenced by the use of social networking.

Technological advancements in the Web have created user friendly and easy to use interfaces and services. Web 2.0 including social media now provide easy environments that permit sharing documents, videos and audio, create groups, add online friends, post profiles, etc. Some configurations also permit to perform these jobs anonymously. This flexibility in the configuration can risk its users to unintentionally violate privacy, intellectual property and other regulations or make actions that may be illegal. Social media permits its users to create their detailed profiles including personal information, relationships, pictures, etc. which can be seen by others and then rearranged and transformed to unacceptable formats and platforms.

Governments and organizations have created laws and regulations that describe what is “right” and what is “wrong” when communicating online. Legal frameworks vary considerable from country to country but the social media has a global character. In many cases appropriate punishments are set to be awarded for violation of these laws. Since Web 2.0 is rapidly changing, therefore, legal frameworks need to be updated frequently to take care of these new developments. However, since in social networking environment different stakeholders share different positions and perform changing roles, it may be difficult to establish responsibility. Further, with little or no knowledge of the laws governing use of social media and consequences for violating some of these laws, users can easily get trapped into crimes for indulging in online offences and crimes.

Attacks through techniques like spear phishing, social engineering and web applications to social media risk individuals, agency, employees and information. Using social media with little or moderate computing skills, individuals or employees face multiple risks from highly skilled cyber attackers to get involved in unlawful activities and compromise on information security and privacy.

5. Social Media Policy and Guidelines for e-Governance

Social media tools have created opportunities for collaborative government and have the potential to facilitate governments to reach its citizens, shape online debates and e-participation, empower citizens, groups and communities and even revive or demand democracy and thus take the evolution of e-government towards new directions. Social media applications also pose several risks including isolation, exclusion, violation of privacy, misuse of information and security threats. Therefore, a comprehensive policy framework can serve as a key enabler for government organizations in providing guidelines for use of social media in governess. Unique challenges are involved in devising policies for the use of social media in e-government as ambiguity looms large on several key parameters including expected benefits, risks involved, effectiveness, etc. Therefore, many government departments throughout the globe have designed guidelines and policies for the use of social media in e-governess projects which differ primarily on the elements covered under these documents and the magnitude of detail under each element. The highlights of a detailed analysis [21] in terms of content and approach of 26 such documents and a limited survey of the use of social media tools by 32 government professionals is presented below:

- Eight essential core elements for a social media policy are: Employee Access, Account Management, Acceptable Use, Employee Conduct, Content, Security, Legal Issues and Citizen Conduct.
- Only five documents addressed the issue of employee access to social media sites, most of them suggested employee access to be controlled by granting access to selected sites only after business case justification.
- Twelve documents addressed the issue of account management, out of which eight were from local governments' which provided explicit policy for account management and others which were state policies provided enterprise level suggestions which varied from one other considerably.
- Twelve documents addressed the issue of acceptable use particularly for personal use. The guidelines mostly pointed to the use of existing acceptable use policy regarding ICT infrastructure. It is clear that the policy makers are striving hard to draw boundaries between personal and professional use of employees.
- Twenty one documents set guidelines for employees conduct addressing issue of employees' behavior which mostly referred directly or indirectly to the general pre-established employee code of conduct. Some provided guidelines specifically to social media including guidelines to respect rules of venue, respect transparency and openness in interactions, and trust. No policy document directly recommended penalties for hosting or disseminating of inappropriate or illegal content.
- Fourteen documents addressed the issues pertaining to content and its management by providing varying guidelines in this regard. Some permit only public information officers or selected individuals or agency functionaries to post content while others permit all employees to post information on agency blogs. No policy provided content guidelines for professional or personal use. Ten policy documents contain instructions to provide a standard disclaimer to announce that employees' opinion and content may not confer to the agency position.
- Fifteen documents provided one or more specific guidelines mostly technical and behavioral to ensure security of data and technical infrastructure of the agency. Some pointed to the use of existing IT security policy. Various concerns pertaining to technological guidelines addressed in these policies included password security, functionality, use of Public Key Infrastructure for authentication, virus scans, use of complex passwords, restriction for posting of classified information, and control of account credentials. The concerns addressed in some documents included spear phishing, social engineering, posting of classified and citizens' information.
- Some of the documents specifically pointed to existing laws and on the contrary others took a general approach suggesting employees to adhere to existing laws and regulations without pointing to the actual laws. The explicitly mentioned laws pertain to privacy, freedom of speech, freedom of information, public record management, public disclosure and accessibility. A few address potential legal issues by directing use of disclaimers of various forms on the social media sites.

- Eleven documents addressed issue of citizen conduct primarily by providing guidelines for dealing with comments posted by citizens. Some allow posting of comments by citizens while others do not. Those allowing posting of comments provide rules referring to offensive language, inciting violence, or promoting illegal activities. Among these some suggest to designate responsibility for controlled flow and moderation of comments.

6. Essential Core Elements of a Social Media Policy

The core elements of a social media policy as identified in [17] are shown in **Figure 2**. Each of the element covers a set of issues that must be addressed to adequately in any successful social media policy for government agencies. These core elements and the issues under each are briefly stated below:

Employee Access: At work employees can use social media sites for the purposes of carrying out official business or professional development or any personnel interests. Access to social media sites can be controlled by different forms of filtering. Controlling access to social media sites of different types of employees performing different roles in an organization is critical for the effectiveness of e-governance. Employee access to social media sites may be controlled by limiting it to some number or type of employees or by limiting the sites or both.

Account Management: Account management in an agency is not only required to keep record of social media accounts created, maintained and closed by its employees for work or professional use but also to define procedures for creation of such accounts. Account Management policy for use in a government agency must clearly be defined as an account gives access to all features of that social media site. An official account on a social media site can be granted by approval of one designated officer or by approval of more than one designated officers.

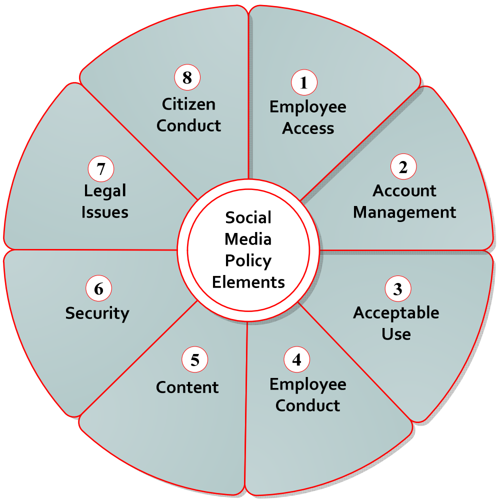


Figure 2. Eight essential core elements of a social media policy.

Acceptable Use: Acceptable use policy governs not only the use of social media but also the use of Internet and other technologies by the employees. It may, quantify online hours, usage monitoring, penalties for policy violation, etc.

Employee Conduct: Employee conduct policy governs, employee online ethics, behavior and penalties awarded for violating this policy. General code of conduct of employees within a government agency to differentiate between “right” and “wrong” in terms of employees conduct may not cover fresh issues associates with social media. Therefore, code of conduct policy for employees governing social media must be revised periodically to cover fresh issues.

Content: Content policy controls permission to employees to post and manage content on official social media pages. It must also govern what type of official content is allowed to be posted on employees’ personal or professional social media page.

Security: Security guidelines aim to safeguard government data and technical infrastructure associated with use of social media from technological and behavior risks. Social media when used in e-governance involves fresh security and privacy concerns which a successful policy must address to adequately.

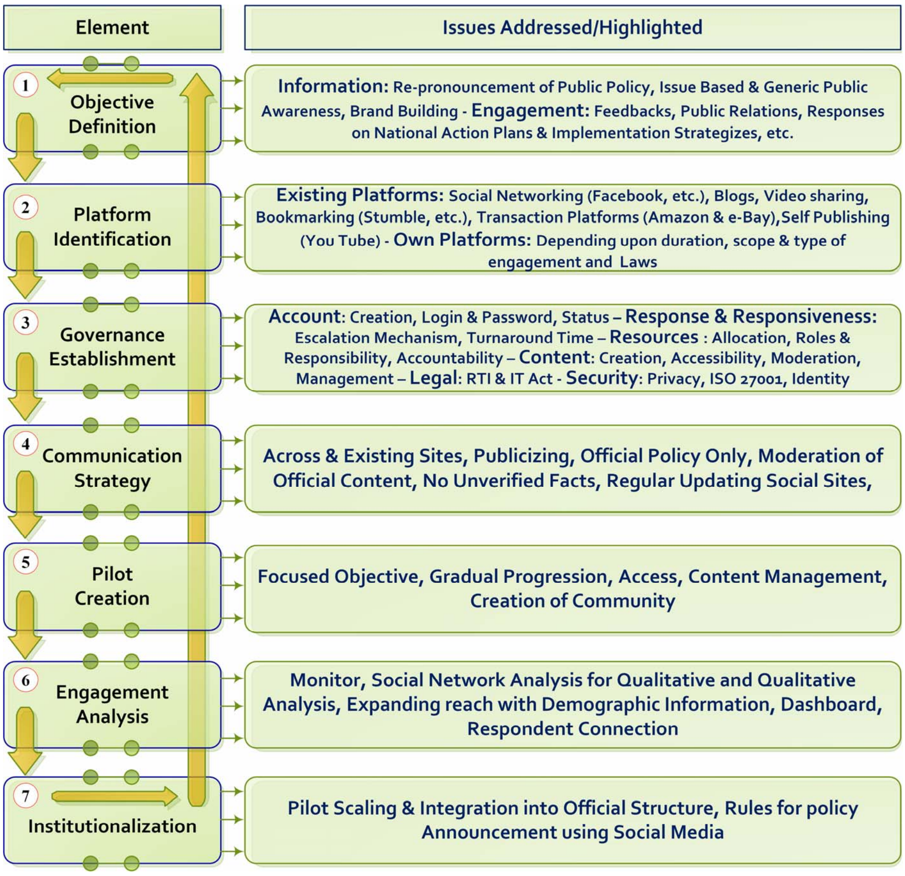
Legal Issues: Legal guidelines ensure that government employees abide by existing laws and regulations when using social media tools. In recent years governments have raised laws regulating Information Technology use by individuals and organizations. However, social media has created possibilities for unique technological, behavior, and social crimes which may not be directly covered under existing laws, therefore, existing Information Technology related laws need to be constantly augmented to check new crimes.

Citizens Conduct: Since social media integration with e-governance makes it possible to have a public citizen-government communication, therefore, rules for citizen engagement with the government are created. These rules govern various aspects of feedbacks and comments including whether to allow comments and feedbacks or not, penalties for use of offensive language, inciting violence and promoting illegal activity.

7. Indian Government Framework & Guidelines for Use of Social Media in e-Governance

In India, various policy/frameworks, standards, guidelines and best practices have been devised for e-governance and several committees such as Metadata and Data Standards (MDDS), Biometrics, Localization, Security, Mobile Governance, Interoperability Framework for e-Governance in India (IFEG), Digital signature, etc. have been constituted to formulate standards. In September 2011, Govt. of India formulated a draft framework and guidelines which has been updated in April 2012 for the use of social media for government organizations [22]. The guidelines aim at assisting e-governance projects of the central and state governments being implemented under national e-governess plan for engagement of social media in these projects. The document briefly introduces social media, its need in government agencies besides providing framework and guidelines for its use. The framework comprises of seven elements which group various issues related to the use of social media sites. Some of the issues are highlighted only while as for others detailed guidelines are provided in this document. These elements and important issues in each of the element are depicted in **Figure 3**. Following sections briefly present various highlights of this framework:

- The framework comprises of seven stages representing seven elements connected in a cycle to demonstrate continuous evolution and scope for improvement. Some issues have been addressed at multiple stages.
- Social media may be used by government agencies for either information dissemination or for public engagement. These include its use for policy making, education and recruitment.
- Existing social media platforms such as social networking, social bookmarking, self-publishing, transaction oriented, or any similar media may be used by government agencies. Agencies may also create their own social communication platforms provided that the existing laws permit it and considering the duration, type and scope of public engagement intended to be offered.
- Official pages on the social media must reflect official position and the interaction must adhere to rules and abide by existing laws with regard to account governance, responses, resource utilization, roles and responsibilities, accountability, content creation, accessibility and moderation, record management, data security and privacy and identity of employees.
- A government agency must maintain same and meaningful name on different social media sites (as far as possible) and proper record of login ID's and passwords. Though, employees' engagement may be



Element	Issues Addressed/Highlighted
1 Objective Definition	**Information:** Re-pronouncement of Public Policy, Issue Based & Generic Public Awareness, Brand Building - **Engagement:** Feedbacks, Public Relations, Responses on National Action Plans & Implementation Strategizes, etc.
2 Platform Identification	**Existing Platforms:** Social Networking (Facebook, etc.), Blogs, Video sharing, Bookmarking (Stumble, etc.), Transaction Platforms (Amazon & e-Bay),Self Publishing (You Tube) - **Own Platforms:** Depending upon duration, scope & type of engagement and Laws
3 Governance Establishment	**Account**: Creation, Login & Password, Status – **Response & Responsiveness:** Escalation Mechanism, Turnaround Time – **Resources** : Allocation, Roles & Responsibility, Accountability – **Content**: Creation, Accessibility, Moderation, Management – **Legal**: RTI & IT Act - **Security**: Privacy, ISO 27001, Identity
4 Communication Strategy	Across & Existing Sites, Publicizing, Official Policy Only, Moderation of Official Content, No Unverified Facts, Regular Updating Social Sites,
5 Pilot Creation	Focused Objective, Gradual Progression, Access, Content Management, Creation of Community
6 Engagement Analysis	Monitor, Social Network Analysis for Qualitative and Qualitative Analysis, Expanding reach with Demographic Information, Dashboard, Respondent Connection
7 Institutionalization	Pilot Scaling & Integration into Official Structure, Rules for policy Announcement using Social Media

Figure 3. Indian government framework for social media.

through personal or official accounts but the official responses should be short and to the point through non-anonymous official accounts and by the cerned official only within pre decided turnaround time. A mail integration may be used to ensure timely response. In case an employee posts comments in personal capacity, it must be ensured that no confidential information is disclosed and the engagement clearly mentions that the comment is personal and not official. Answers to frequently asked queries should be prepared, maintained and displayed for which no separate engagement should be encouraged. Social media must be used for propagation of only official policy and no unverified information or frivolous material should be posted.

- Resources for social media and their responsibilities may be either outsourced or internal to an agency. For moderated conversation, it is necessary to have dedicated resources including a well-trained leader within the agency. There must be clearly defined roles and responsibilities set with regard to responding of Right to Information (RTI), maintenance of IDS and passwords, data security, privacy, etc. Employee should be accountable for their use of social media and employee engagement must be governed by RTI Act, IT Act 2000 and IT Amendment Act 2008.
- Official content must be specified, tailored, moderated and must follow Government of India guidelines for Websites, address challenges related to accessibility of Indian languages and differently abled persons. Records of interactions influencing decision making must be preserved in soft/hard copies. Agencies are encouraged to enter service level agreements with social media service providers to ensure Indian regulations for storage, archiving, access, complaint and response mechanisms.
- All existing laws more particularly RTI Act, IT Act 2000 and IT Amendment Act 2008 govern the engagement on social media. Security of personal data is governed by Information Technology (Reasonable Security Practices & Sensitive Personal data or Information) rules 2011 and ISO 27001 standards. Privacy of individuals must be guaranteed in accordance to existing laws governing data protection and privacy.
- A pilot must be created to test the efficiency and effectiveness of the engagement with public. The engagement must be quantitatively and qualitatively monitored using social network analysis and demographic information, dashboards and respondent connection must be used to extend and expand the engagement. After successfully refining the pilot it must be scaled and fully integrated in the agencies communication and administrative structure.

8. Limitations of Indian Government Guidelines for the Use of Social Media in e-Governance

Though this framework and guidelines have been revised in April 2012 after its initial preparation, yet there are various issues that either have not been fully addressed to or have not been included in the guidelines. The shortcomings in the framework are enumerated below:

- Neither any clear guidelines regarding employees' permission to access social media sites during office hours for their professional and personal use nor any technological measures such as filtering has been suggested for controlling employee access to these sites in the framework. The objective of the use of social media in government organizations does not include use of social media for employee professional and personal development. Further, the guidelines does not include any instructions regarding the mechanism for granting controlled access (business case justification, access to selected sites, duration of access, etc.) to employees to social media sites for official purpose.
- Though Account management has been covered by the guidelines but certain issues like procedure for granting permission to an official to procure an official account on social media site have not been discussed. A public information officer in most of such policies is made in charge of granting such a permission. For a strict control often approval from two parties like communication department and IT department has been suggested.
- The resource governance sub section of the policy covers acceptable use which does not directly quantify online hours, usage monitoring, penalties for policy violation, etc. However, it suggests that the employee allowed to interact with the public should be held accountable and points out at existing immunity provision of RTI Act, IT Act and IT Amendment Act 2008. Further, like some other policies and documents, it has not drawn boundaries between personal and professional use of employees.
- Guidelines for employees conduct have been given at multiple places in the document which are in tune with such guidelines provided in other policy documents. Detailed guidelines have been provided for legal provisions in this regard. Since social media provide 24X7 engagement opportunity, the guidelines fall short in addressing employee conduct from professional and personal accounts.
- Guidelines for the employees to post in personal or professional capacities have not been addresses to in the framework. Guidelines do mention requirement of moderation of the content, however, does not provide sufficient guidelines for fixing responsibilities within

the organization for this purpose. Various policies permit their employee to post freely on agency blogs on various mission related topics but Indian guidelines are silent in this regard.

- The framework has provided guidelines for security of personal data and also has covered privacy of individuals, however, it lacks technical guidelines for achieving the same. No guidelines have been provided for password security, functionality, use of PKI for authentication, virus scans, use of complex passwords, and control of account credentials. It does not provide guidelines for spear phishing or social engineering.
- Legal guidelines have been provided at multiple places in the framework, however, all of them repeat the existing laws that include RTI Act, IT Act, and IT Amendment Act 2008. Though, most of the issues are covered by these laws but social media has created possibilities for unique technological, behavior, and social crimes which may not be directly covered under these laws, therefore, existing Information Technology related laws need to be constantly augmented to check new crimes.
- With respect to the citizen conduct, rules have been clearly depicting how a government agency should classify comments and engage with the citizens. They specify who and when it is necessary and not necessary to respond to comments. Further, they also specify why and how comments that make influence on the policy making decision should be preserved. However, the policy is silent about mechanism that could make a public comment or feedback acceptable or not for the purpose of policy making, etc.
- The guidelines are silent about information confidentiality, integrity and availability and procedures government agencies should adopt to achieve this trio. Though the policy refers to the adherence of various sections of IT Act 2000 and its amendment but no direct reference has been given to any information security act or standard. ICT faces severe security challenges but no specific or very limited guidelines are provided for information security education.
- The guidelines fall short to address risk management, mitigation and issue of acceptance of residual risks by the use of social media. Though the guidelines encourage agencies to enact service level agreements with operators of social media sites but do not provide guidelines about what agencies should seek from these operators in respect of stronger security and privacy controls, multifactor authentication, cross site scripting, persistent cookies, content moderation and monitoring, access to employees official accounts, and code validation and signing.
- The guideline does not provide emphasis on periodic awareness and training of security, policy, best practices for social media. Further, it does not instruct agencies to periodically and constantly update their social media policy especially with respect of privacy & security, content filtering, and acceptable use.

9. Recommendations for Improvement

The Web 2.0 Security Working Group (W20SWG) responsible for accessing information security issues surrounding Web 2.0 technologies in the Federal Government of USA has provided Guidelines and recommendations for using social media technologies in a manner that minimizes the risks involved in it [20]. The document encourages use of social media in government agencies on a strong business case and following adequate security guidelines. The recommendations include five categories of controls grouped into technical and non-technical controls. The technical controls are network and host controls and the non-technical controls are policy controls, acquisition controls and specialized trainings. These security controls should be adequately adapted to make integration of social media in e-governance secure.

The policy document for the use of social media in e-governance must include guidelines to achieve confidentiality, integrity and availability of information and data. It must provide guidelines for the use of various network security control measures including the use of trusted Internet connection, intrusion detection system, intrusion prevention system, Web content filtering methods like traffic filtering and deep packet inspections, creation of security zones, use of domain name security, multi-facet authentication and other emerging security technologies. Clear instructions must be included for the acquisition of social media services and service level agreements for acquisition of enhanced security, privacy and monitoring controls. Proper risk assessment and acceptance of residual risk must be made through some third party before deciding on the use of a particular social media service which must be reassessed periodically. Incorporating social media in e-governance especially in developing countries like India must necessarily include guidelines for security training and assessment of employee technical skills before granting access to social media sites for official purposes.

Different government agencies may require different employee access policy and thus a uniform access policy may not be fit for all government agencies. E.g. In an academic or research functionary of a government where employees are engaged in collaborative and knowledge sharing activities and employees' professional development is vital to the development of organization access to specific social media sites may be desired. Therefore, policy must be flexibility to enable agencies to permit use of social media during office hours for professional developments wherever applicable. In such a case improvement in accountability system are desired which may be in the form of maintenance of log of all online activities undergone during the office time. The policy must include strict instructions for widely publicizing of all its social media accounts to control any confusion amount its users. The work account must be used for only official work and should always remain a property of the agency and must be open for inspection and surrendered on transfers or retirements. State and local government policies vary on scale and the level at which account management issues are addressed to and therefore, may differ considerably on management of social media accounts. Acceptable use policy must set boundary around professional, personnel and agency use of social media tools. The existing standard code of conduct followed in government agencies do not address issues involved in employee online conduct especially when using social media tools. Therefore, a successful social media policy must directly address fresh issues of employee conduct associated with the use of social media. To avoid inconsistency between content on social media pages and other electronic and print media pages of the agency, the social media policy must contain strict rules and well defined penalties for its violation. Specific guidelines are to be devised for preparation of e-content, authentication; integrity and non-reputation of e-content and liability of authors needs to be defined.

10. Conclusion

Advantages of social media like collaboration, participation, and empowerment have attracted governments to use it in governance for bringing together agencies, citizens, agencies work and information. It is used to promote e-services, increase transparency and improve trust on government. Persistent, pervasive and aggressive threats are faced by government information systems which gets intensified through the environment created by social media as it involves risks on multiple fronts including those related to behavior, ergonomic configuration, regulation and technology. When used in e-governance, social media may also poses risks of isolation, exclusion, violation of privacy, misuse of information and security threats. Therefore, governments have devised comprehensive frameworks, policies, guidelines and best practices to serve as key enabler for government organizations for the use of social media in governess. Different policies give emphasis on different elements and mostly point to the adherence of existing laws and regulations for securing data and information. Some policies suggest that the decision to incorporate social media in e-governance at an agency should be supported by strong business justifications but with adequate security and privacy controls while as others consider it necessary for inclusion or do not provide adequate guide- lines for security and privacy of data. Indian government framework is in tune with other such policies and also includes policy for its multilingual cultural. However, it does not include guidelines for all identified core elements or does not provide sufficient guidelines to some of the parameters that a successful social media policy should have. There is a scope for improvement in each element included in this framework more importantly in the guidelines pertaining to security controls, acquisition of third party services, risk assessment, employees training, account management and legal.

REFERENCES

[1] Human Capital Institute, “Social Networking in Government: Opportunities and Challenges,” 2012. http://www.hci.org/files/field_content_file/SNGovt_SummaryFINAL.pdf

[2] T. D. Susanto and R. Goodwin, “Factors Influencing Citizen Adoption of SMS-Based e-Government Services,” *Electronic Journal of E-Government*, Vol. 8, No. 1, 2010, pp. 55-71.

[3] United Nations, “e-Government Survey,” 2012. http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf. ISBN: 978-92-1-123190-8

[4] R. Reffat, “Developing a Successful e-Government,” Working Paper, School of Architecture, Design Science and Planning, University of Sydney, Sydney, 2003.

[5] Z. Fang, “e-Government in Digital Era: Concept, Practice and Development,” *International Journal of the Computer, the Internet and Information*, Vol. 10, No. 2, 2002, pp. 1-22.

[6] W. Darrell, “US State and Federal e-Government Full Report,” 2002. http://www. insidepolitics.org/egovt02us.pdf

[7] N. Sampson, “Bank Marketing International: Simplifying in (Form)ation,” 2002. http://www.mandoforms.com/news/coverage/bankmarketing.html

[8] A. Kurunananda and V. Weerakkody, “e-Government Implementation in Sri Lanka: Lessons from the UK,” *Proceedings of* 8*th International Information Technology Conference*, Colombo, 12-13 October 2006, pp. 53-65.

[9] F. Bélanger and L. Carter, “The Effects of the Digital Divide on e-Government: An Empirical Evaluation,” *Proceedings of the* 39*th Hawaii International Conference on System Sciences*, Vol. 4, 2006, pp. 1-7.

[10] D. H. McKnight and N. L. Chervany, “What Trust Means in e-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology,” *International Journal of Electronic Commerce*, Vol. 6, No. 2, 2001-2002, pp. 35-59.

[11] F. V. Morgeson, D. Van Amburg and S. Mithas, “Misplaced Trust? Exploring the Structure of the e-Government-Citizen Trust Relationship,” *Journal of Public Administration Research and Theory*, 2010.

http://www.terpconnect.umd.edu/~smithas/papers/morgesonetal2010jpart.pdf

[12] T. S. H. Teo, S. C. Srivastava and L. Jiang, "Trust and Electronic Government Success: An Empirical Study," *Journal of Management Information Systems*, Vol. 25, No. 3, 2008-2009, pp. 99-132.

[13] E. W. Welch, C. C. Hinnant and M. J. Moon, "Linking Citizen's Satisfaction with e-Government and Trust in Government," *Journal of Public Administration Research and Theory*, Vol. 15, No. 3, 2005, pp. 371-391. doi:10.1093/jopart/mui021

[14] B. Shah, "Increasing e-Government Adoption through Social Media: A Case of Nepal," Örebro University, Swedish Business School at Örebro University, Örebro, Sweden, 2010. http://oru.diva-portal.org/smash/get/diva2:372485/FULLTEXT01

[15] Y. Charalabidis and E. Loukis, "Transforming Government Agencies' Approach to e-Participation through Efficient Exploitation of Social Media," *ECIS* 2011 *Proceedings*, Paper 84, 2011. http://aisel.aisnet.org/ecis 2011/84.

[16] J. Michael Magro, "A Review of Social Media Use in e-Government," *Administrative Science*, Vol. 2, No. 2, 2012, pp. 148-161. doi:10.3390/admsci2020148

[17] J. Hrdinova, N. Helbig and C. S. Peters, "Designing Social Media Policy for Government: Eight Essential Elements," Center for Technology in Government, University at Albany, 2010. www.ctg.Albany.edu

[18] D. Landsbergen, "Government as Part of the Revolution: Using Social Media to Open Government," Ohio State University, Columbus, 2010.

[19] D. Landsbergen, "Government as Part of the Revolution: Using Social Media to Achieve Public Goals," *Electronic Journal of e-Government*, Vol. 8, No. 2, 2010, pp. 135-147.

[20] C. I. O. Council, "Guidelines for Secure Use of Social Media by Federal Departments and Agencies," Federal CIO Council ISIMC NISSC Web 2.0 Security Working Group, 2009, pp. 1-19.

[21] P. Trudel, "Web 2.0 Regulation: A Risk Management Process," *Canadian Journal of Law and Technology*, Vol. 7, No. 2, 2010, pp. 243-265. http://cjlt.dal.ca/vol7_ no2/pdf/trudel.pdf

[22] DEIT, "Framework & Guidelines for Use of Social Media for Government Organizations," Department of Electronics and Information Technology, Government of India, 2012. http://www.negp.gov.in/pdfs/Social%20Media%20Framework%20and%20Guidelines.pdf