Social Networking and e-Government: The Role & Its Impact

Ramandeep Kaur, Dipen Saini

Abstract— **The emerging multiple technological developments in communication and information technology have started a new gateway for the effective form of communication in terms of social networking sites. Nowadays, there are various online applications of social media to enable communication between groups, people. This research paper makes an effort to analyze the recent utilization of social media as well as their bright edges for e-governance in various government organizations or sectors. It discusses prospective problems particularly problems related to the privacy and security of employees, individuals, data and infrastructure that hinder the successful execution of social media for e-governance. It analyzes the framework of government of India for including social media in executive or governmental structure. It analyzes issued guidelines for different platforms to be employed, authorization to participate on behalf of the governmental organization, extent, and scope of such engagement, etc. This paper compares the issued guidelines with the related guidelines of other countries in terms of account management, employee's access, employee conduct, acceptable use, security, content, legal problems, and citizen conduct and it also enumerates its scope, merits, and demerits for further improvements.**

***Index Terms*— Social Media Framework, Social Media, e-Governance, Social Media Policy, Social Networking**

I. INTRODUCTION

Social networking gives users with profound and rich experience for interaction, participation, and collaboration. Different social media tools enable their users to share and create information/data on the web and work together with others interactively hence making easier to locate information and connect and communicate online with each other. Social media has likewise been utilized for e-learning as they've created various opportunities for effectual teacher-teacher, learner-learner and teacher-learner communication, collaboration and interaction. With the advancement of mobile technology, there's not been powerful in the type and a number of social networking or media tools, however, the utilization of these tools is also on the increase. In fully developed countries like Poland, USA, Korea and the UK at least 4 out of 10 adult citizens utilize various social media applications. Social media websites dominate the usage of Internet in the Pacific and Asia [1]. In contrast with males, females are more enthusiastically engaged in different social media websites [2]. However presently the utilization of social media websites is more well-liked among grown-ups but various studies are showing that there is an emerging trend of participation by elders as well from last few years. Generally social media can be characterized in the accompanying four classes:

1. Online networks—such as Twitter, Facebook, MySpace, and LinkedIn
2. Online publication tools—such as Flicker, YouTube, RSS, Twitter and SlideShare
3. Online collaborative applications/platforms —such as Wikis, for example, MediaWiki, blogs, for example, Blogger or Wordpress, and collaborative office solutions such as Google Docs, Office-365, Debategraph, MS Lync, WorkSpot or Teamwork, and
4. Online feedback Applications—for example, debating and voting, commenting and rating, polls, surveys, blogs, and so forth.

Online networks as well as ecosystems develop and represent the networks and also relationships among peers. Online publication platforms provide services for publishing and sharing content online. Online collaborative platforms give the flexibility to work effectively with different people. Online feedback tools take input from the audience through 1-way or 2-way communication. To advertise and promote business, several organizations have embedded social media in their structure. Legislatures of different countries have also included social networking in e-governance, but, in order to make this type of integration efficient and more secure they've devised policies, frameworks, and guidelines that direct this integration.

The rest of the paper is organized as Section 2 spotlight on the utilization of the social networking in e-governance. This paper also discusses its potential benefits and involved dangers in Sections 3 and Section 4 correspondingly. Section 5 shows the highlights of a most recent study which examined 26 social networking/media documents. Section 6 enumerates the various core elements of the effective social media policy. In Section 7, Indian Government guidelines and framework related to social media with respect to e-governance are analyzed and its limits are discussed in Section 8. At last, Section 9 gives guidelines for enhancing this framework or system followed by the conclusion.

II. PROCEDURE FOR PAPER SUBMISSION

Academic institutions, commercial organizations, and individuals utilize social media broadly for online presence, services, and goods promotion, collecting feedbacks from the customer, experience sharing, customer and consumer interactions, preparation of collaborative content, e-learning, social interaction, communication, etc. Recently, governments, citizens, and politicians throughout the world also including those who are from least developed nations

Manuscript received March, 2016.

Ramandeep Kaur*, Post Graduate Department of Computer Science, D.A.V. College, Jalandhar, Punjab, India.*

Dipen Saini*, Post Graduate Department of Computer Science, D.A.V. College, Jalandhar, Punjab, India..*

ISSN: 2278 – 1323

have exhibited the effective utilization of social media apps and tools to transform governance arrangements, holding election campaigns, mobilize movements in and against governments, sustain government-to-citizen communication and interaction in disorder, and so on. Mitt Romney and Barack Obama have actively adopted Twitter and utilized the social networking websites as their campaign resources in the 2012 presidential contest in order to interact directly with different supporters and, more significantly, make the political conversation in such a manner that reaches far away from the website. Government officials or governments under some kind of policy in their personal competence have been utilizing social networks for information, administration and foreign affairs. The UK and USA authorities beside others such as Sweden and Australia are most dynamic in the utilization of social networking for digital diplomacy. Presently, 66% of all the agencies of USA Government use various forms of social media site [1]. As per the survey of the UN e-Governance 2012 [3], 48% that is, 78 affiliate states give either a "follow us on Twitter" or "follow us on Facebook" statement on their legitimate governmental websites. This survey also highlights that 7% of such sites provide IM features or chat rooms to collect public opinion. In India also, various officials and ministers actively utilize social media to interact and communicate with citizens.

III. Benefits of Utilizing Social Media/Networking in e-Governance

A variety of impediments to e-governance adoption includes lack of e-service awareness [4], accessibility to e-services[5-6], various interest related to citizens [7], government support [8], low utilization of government sites and digital divide [9]. Another significant factor in the adoption of cutting-edge technologies needed in e-governance is the government trust. Interaction with citizens continues to be acknowledged as the most effective measure to establish this faith towards e-governance [10-13].

The 4 noteworthy potential strengths related to social media websites are

1. Participation,
2. Collaboration,
3. Time, and
4. Empowerment.

These aid governments to serve its citizens as they promote and advertise government services, information, and cooperation with its partners bringing together citizens, government agencies, agencies work and info. Social media can increase the Internet usage to realize the packed advantages of e-governance. Web sites of social media not only give advantages to e-governance by monitoring and intensifying services however also reduce the costs whilst enhancing their quality. Utilizing these websites, governments can easily publish job advertisements, advertise and promote different services, market events, search for public feedbacks and collaboration and pool resources across its geologically diverse agencies. As social media has the giant prospectus for growing citizen utilization of e-service [14] as well as e-participation [15], its noteworthy usage by the community could boost transparency which then can boost government trust. A current review [16] about the usage of social media in e-government has demonstrated its several other benefits in e-governance. In its current report labeled with "Designing Social Media Policy for Government: Eight Essential Elements" in [17] 3 diverse ways of utilization of social media websites by different employees at the workplace have been recognized by "Centre for Technology in Government, University at Albany". These specific uses are for personal interest, professional interests, and official agency interests. These 3 aren't mutually exclusive and at times, there are no clear-cut lines separating the official agency usage from professional usage or professional usage from personalized use. David Landsbergen [18, 19] in his current research works recognized ways in which various social media applications or tools are utilized in several government agencies and gathered 5 mechanisms as described in Figure 1.

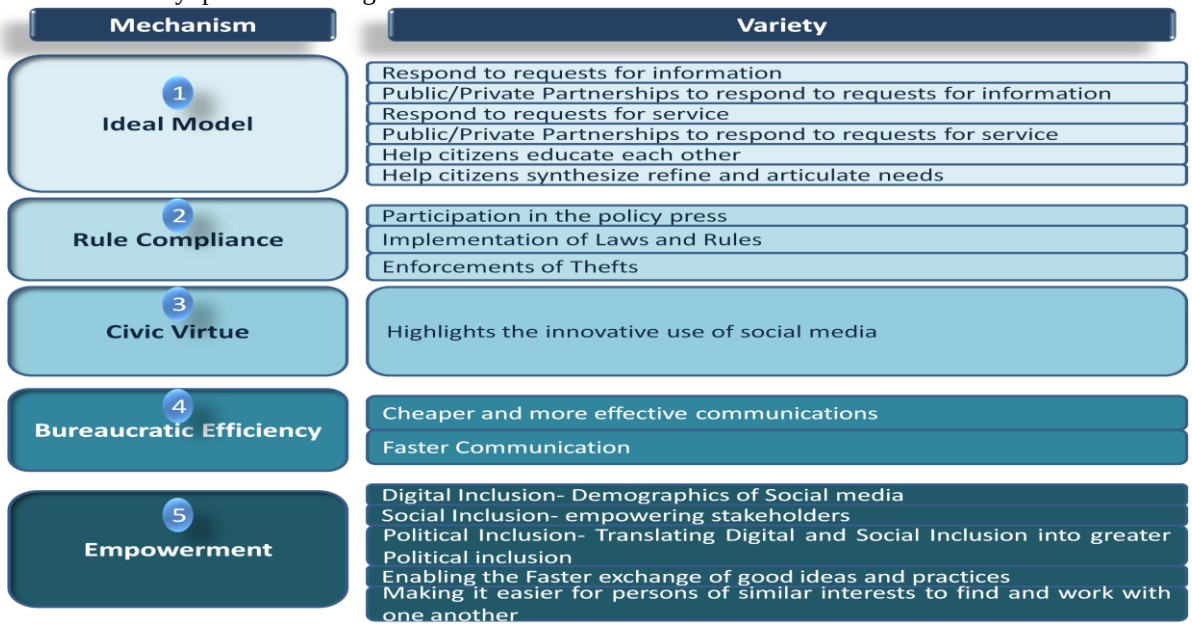

Figure 1 Mechanism through Which Social Media Tools Realize Government

ISSN: 2278 – 1323

IV. Risks involved in the Utilization of Social Media for e-Governance

Governmental information systems together with its individuals, infrastructure, employees, agency, and information are confronting threats which are aggressive, pervasive and persistent [20]. This type of situation gets intensified by the surrounding built by social media as it utilizes Web 2.0 technologies which are relentlessly changing and includes risks on different fronts incorporating those related to ergonomic configuration, behavior, technology and regulation [21]. As the involved risks are interdependent, so, controlling the one might intensify the other.

As the Web 2.0 environment facilitates its users with the gigantic power to interact, share and collaborate, they can simply indulge in several practices which could violate the other's rights. The most general risks identified with the conduct of users amid interactions on the Internet are risks to privacy, reputation, publication to illegal and personal content and intellectual property. Social media has its own potential to boost campaigns against or in favor groups or governments. There is a vile utilization of social networking tools too, for example during summer 2011 riots in the United Kingdom. In Kashmir, 2011 rise of separatist movement creating unrest in the Kashmir was likewise directly impacted by the utilization of social networking.

Different technological advancements on the Web have created user-friendly and easy to use interfaces and services. Web 2.0 incorporating social media presently facilitate easy environments which permit sharing audio and videos, documents, add various online friends, create groups, post profiles, and so on. A few configurations also let you perform these types of jobs secretly. This particular flexibility in the social media configuration can risk its visitors or users to unintentionally breach intellectual property, privacy and another sort of regulations or make actions that may be illegal. Social media allows its users to make their detailed profiles incorporating including relationships, personal information, pictures, et cetera that can be observed by others and after that transformed and rearranged to unacceptable platforms and formats.

Governments and organizations have designed various rules and regulations which describe what is "good" and what is "bad" while communicating via web. Legal frameworks vary considerably from state to state however the social networking has a universal character. In many cases, different punishments are set to be awarded for violation of these laws. As Web 2.0 is rapidly transforming, so, legitimate frameworks need to be updated frequently to take care of these new developments. However, since in social media environment several stakeholders share various positions and implement different roles, it can be too much difficult to set up responsibility. Further, with little or no knowledge of the laws which governs the use of social media and various consequences for breaking some of these laws, users can very easily get caught into offenses for indulging in different online crimes and offenses.

Attacks which are implemented with techniques like social engineering, spear phishing and web apps to social media directly harm individuals, employees, agency, and information. Utilizing social media with moderate or little computing skills, employees or individuals face multiple types of risks from skilled and proficient cyber attackers in order to get mixed up in illegal activities and compromise with the information privacy and security.

V. Social Media Guidelines and Policy for e-Governance

Social networking tools have developed different possibilities opportunities for collaborative authorities. Social media also have the ability to ease governments to approach its citizens, create online debates and forums as well as e-participation, and empower communities, groups, and citizens. So, in this way, social media take the advancement of e-government in new directions. Social networking programs also prevent several risks incorporating exclusion, isolation, privacy violation, and information misuse and security threats. So, a complete policy framework can work as an enabler for different government organizations by offering guidelines for the utilization of latest social media tools in governess. Different challenges are included in formulating policies for social media use in e-government as part of the ambiguity looms on various key parameters incorporating expected benefits, effectiveness, risks involved and so forth. So, several government departments across the world have designed policies and guidelines for the utilization of social networking in e-governess recent projects which differ only in elements which are covered in these documents. The things that need to be considered in the detailed analysis [21] as per content of 26 such type of documents and a small survey of social media tools utilization by 32 government experts is listed beneath:

- The eight important core elements included in the social networking policy are Account Management, Employee Access, Employee Conduct, Acceptable Use, Security, Content, Citizen Conduct and Legal Issues.
- Only 5 documents addressed the potential problems of employee access to various social networking websites, the majority of them recommended employee access be restricted by allowing access to selected websites only after the business justification process.
- 12 documents addressed the potential problems of account management, among these 12, 8 documents were from local authorities or governments' which supplied explicit and clear policy for the account management and rest documents were state policies which provide different enterprise level suggestions and these differ from one other significantly.
- 12 documents addressed the potential problems of acceptable use, especially for private use. The rules or guidelines generally pointed to the utilization of existing acceptable use of the policy regarding Internet Communication Technology (or ICT) infrastructure. It is also clear that the makers of policy are striving very hard to make boundaries between the professional and personal use of workers or employees.
- 21 documents set up different guidelines for the

ISSN: 2278 – 1323

employees conduct which normally addressing the potential problems of employees' behavior. This mainly sent indirectly or directly to the pre-established employee conduct code. Some offered guidelines particularly to social media incorporating guidelines or rules to respect venue rules, respect transparency as well as openness in communication, and trust. There is no such policy document which directly recommends penalties for disseminating or hosting of illegal or inappropriate content.

- 14 documents addressed the potential problems related to content. The management is done by giving varying guidelines or rules in this respect. Some allow only agency functionaries, selected individuals, and public information officers to post and publish content whilst others allow all employees to publish info on agency websites or blogs. No policy provided content guidelines for professional or personal use. Ten policy documents have instructions which provide a disclaimer to declare that content and opinion of employee may not bestow the agency position.
- 15 files supplied with one or more particular guidelines mostly behavioral and technical to guarantee the security of data as well as the technical infrastructure of the firm. Some indicated the use of existing information technology security policy. Numerous concerns relating to technological guiding principles addressed in these plans or policies included functionality, password security, utilization of Public Key Infrastructure for verification, utilization of complex passwords, constraints on a posting of confidential information, and management of account credentials. The things listed in some documents are social engineering, spear phishing, and posting of citizens' information.
- A few of the files specifically indicated to existing laws took a universal approach signifying employees to stick to existing regulations and laws without pointing to the authentic laws. The laws which are explicitly mentioned are privacy, freedom of information, freedom of speech, public record management, accessibility and public disclosure. Some address officially permitted issues by advising the utilization of disclaimers of different forms on the social networking sites.

Eleven files addressed the various issue of the conduct of citizen primarily by offering guidelines for handling comments published by citizens. Some of the documents enable you to publish comments whilst other documents do not. The documents which allow comment publishing offer rules referring to inciting violence, offensive language, or promoting illicit activities.

VI. Social Media Policy: Important Core Components

The core components of social media guidelines as determined in [17] are described in Figure 2. Every component covers the particular number of issues that should be addressed in any booming social network policy for governmental agencies. The social media policy core components and their corresponding issues are listed beneath:

- *Employee Access*: Employees can utilize social media websites for official business or professional development or personnel interests. Access to such websites can be managed by various types of filtering forms. Managing accessibility to social networks websites of various types of workers performing different roles in an organization is critical for the performance of e-governance. Employee access to social networking websites may be managed by restricting it to some type or number of employees or by restricting the websites or both.
- *Account Management*: Account management isn't only needed to maintain a record of different social media accounts maintained, closed and created by its employees for professional use or work but also to describe procedures for the formation of such social media accounts. Account Administration plan for usage in a federal government firm need to plainly be defined as an account which gives access to all attributes of the social networking website. The official account on the social media website can be accepted only by approval of the chosen officer or can be by approval of different designated officers.
- *Acceptable Use*: The use of this policy governs the utilization of social media and The Internet and various other employees technologies. It may evaluate online hours, monitoring the usage, policy violation penalties, and so forth.

Figure 2 Social Media Policy: 8 Essential Core Elements

- *Employee Conduct*: This policy governs online ethics of employee, behavior & penalties granted for breaching this policy. The general code of employee conduct within the governmental agency to make a distinction between "wrong" and "right" as per the employees conduct might not include the issues associated with social media. So, employees conduct policy should be revised regularly in order to cover the issues.

ISSN: 2278 – 1323

- *Content*: This policy handles permission to different employees to manage and publish content on certified social media web pages. It should also direct what sort of official web content is permitted to be published on employees' professional or personal social media web page.
- *Security:* Security guiding principles aims to safeguard the technical infrastructure and government data associated with the utilization of social networking from behavior and technological risks. Social networking/media, when employed in e-governance, includes privacy and security concerns.
- *Legal Issues:* Guidelines related to this policy ensure that employees of government abide by the existing regulations and laws. Over the last few years, federal governments have elevated laws which generally regulate the Information Technology usage by organizations and individuals. Nevertheless, social networking has designed possibilities for technological, social and behavioral offenses which might not be as such covered under the existing laws, so, IT (Information Technology) related laws have to be frequently enhanced to inspect new criminal offenses.
- *Citizens Conduct*: As integration of social media with e-governance most of the times makes it feasible to have a communal communication of citizen-government, therefore, rules regarding citizen engagement with the government are created. These specific rules govern different aspects of comments and feedbacks incorporating whether to enable feedbacks and comments or not, penalties for utilization of offensive language, advertising illegal activity, and inciting violence.

VII. Indian Government Guidelines & Framework Regarding Social Media in e-Governance

In India, numerous frameworks/policies, guidelines, standards, and best strategies have been designed for e-governance and also several committees like MDDS (Metadata and Data Standards), Localization, Biometrics, Mobile Governance, Security, Digital Signatures, IFEG (Interoperability Framework for e-Governance) in India and so forth have been constituted to plan standards. The government of India designed guidelines and framework in September 2011, which has been actually updated and revised in April 2012 for the utilization of social media in government organizations [22]. The various guidelines target at helping e-governance projects of the state and central governments being implemented or executed under the national plan of e-governess for engagement and interaction of social media in these particular projects. This paper briefly presents social media as well as its need for the governmental agencies. The framework consists of 7 core elements which combine different issues allied to the utilization of social media websites. A few of the issues are discussed. These core elements and potential issues are illustrated in Figure 3.

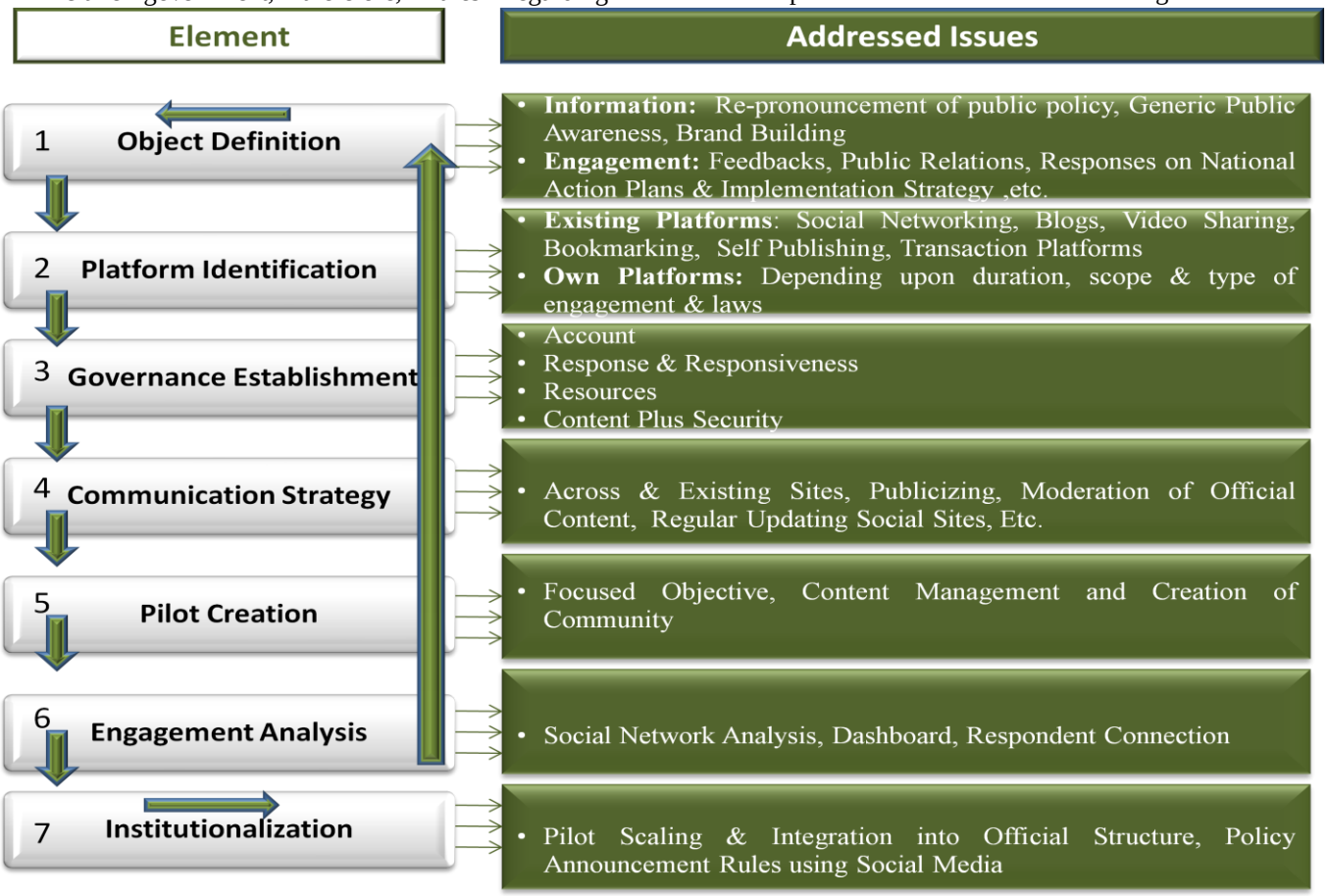

Figure 3 Framework of Indian Government for Social Media

The following section presents several things of the governmental framework:

- The government framework contains seven stages which represent seven elements linked to each other

ISSN: 2278 – 1323

in the form of the cycle to show the continuous evolution as well as scope for development. Some of the issues have actually been discussed and addressed at different stages.

- Social media could be utilized by government agencies for public engagement and for information dissemination. These include policy making, recruitment, and education.
- Existing platforms of social media such as social bookmarking, social networking, transaction-oriented or self-publishing, or any other media might be utilized by government agencies. These agencies might also generate their own platforms of social communication provided that their existing laws allow them.
- Social media official web pages must reflect the official interaction and position need to comply with rules & regulations and abide by the existing laws according to the account governance, resource utilization, responses, accountability, roles and responsibilities, accessibility and moderation, content creation, data security, record management, and identity and privacy of employees.
- A government agency should maintain meaningfully and the same name on various social media websites and proper record management of login ID's plus passwords. Although, the engagement of employees may be with official and personal accounts however the official responses need to be crystal clear and short. The mail integration might be utilized to guarantee a timely response. If an employee publishes comments personally, then it should be ensured that no private info is disclosed. The engagement clearly describes that the published comment is personal and isn't official. Answers to various FAQs should be displayed; maintained and prepared for which no other separate engagement ought to be encouraged. Social networking sites should be utilized for the propagation of the official policy only. Keep away yourself from frivolous material or unverified information and this type of information should not be posted on the site.
- Social media resources and their corresponding responsibilities might be either internal or outsourced to an agency. For general conversation, it is important to get dedicated resources incorporating a trained leader within the government agency. There should be clearly stated roles and responsibilities set when it comes to Right to Information (RTI), maintenance of different IDs and their passwords, privacy, data security and so forth. Employees need to be accountable for their usage of social media. The employee engagement should be governed by IT Amendment Act 2008, IT Act 2000 and RTI Act.
- The official content of websites must follow guidelines of Government of India. Different interaction records influencing the concept of decision making should be preserved in the form of hard or soft copies. Agencies are urged to get agreements at service level with the service providers of social media to guarantee Indian regulations for archiving, storage, complaint, access, and response mechanisms.
- All existing legislations especially IT Amendment Act 2008, IT Act 2000 and RTI Act govern the social media engagement. Personal data security is governed by ISO 27001 standards and Information Technology (IT) (i.e. Reasonable Security Practices & Sensitive Personal data or In-formation) rules 2011. Individual's privacy must be ensured as per the existing laws which govern data privacy and protection.
- A pilot should be designed which test the effectiveness and efficiency of the engagement with the public. The engagement should be qualitatively and quantitatively monitored by utilizing social network demographic information and analysis, respondent connection and dashboards should be utilized to expand and extend the engagement. After efficiently refining the pilot it should be integrated and scaled in the administrative structure and agencies communication.

VIII. Drawbacks of Indian Government Guidelines Corresponding to Social Networking in E-Governance

Though the guidelines and framework have actually been updated in April 2012 right after its initial prep work, but there are several issues which either haven't been included or haven't been fully addressed in these guidelines. The limitations of the framework are listed beneath:

- Neither any sort of clear guiding principles regarding the employees' permission to use the social networking website during their office hours for personal and professional use nor any type of technological measures like filtering has been recommended for handling employee access to these types of websites in the Indian Government framework. The major goal of the utilization of social networking in government agencies doesn't include the utilization of social media for personal development and employee professional. Additionally, the guidelines don't incorporate any instruction regarding the process for giving controlled access (access to selected websites, business case justification, access duration and so forth) to employees to social networking sites for official purpose.
- Although Account management has been properly covered by different guidelines but some of the issues like the process for granting permission to secure an official account on the social networking website haven't been discussed. The officer of public information in most of these policies is generally made in order to grant such type of permission. For a restricted control approval from two different parties like IT department and communication department has been suggested.
- The sub-section called resource governance

ISSN: 2278 – 1323

generally entails the acceptable use that does not quantify the usage monitoring, online hours, policy violation penalties and so forth. However, it recommends that the employee permitted to interact or communicate with the public should point out the existing immunity provision of IT Amendment Act 2008, IT Act and RTI Act. Additionally, like other documents and policies, it hasn't drawn the boundaries between professional and personal employees' use.

- Employees conduct guidelines have been mentioned at different places in the document that are according to such guidelines. The detailed guidelines have also been given for legal provisions in this context. As social media offer 24-by-7 engagement opportunity, these guidelines fail in addressing the employee conduct from personal and professional accounts.
- Guidelines for different employees to publish professional or personal posts haven't been addressed in this framework. Several policies allow their employee to publish a post on the blogs of the agency on different mission-related topics. However Indian guidelines are still silent in this context.
- The framework has offered guidelines for individual's privacy and personal data security, but, it lacks from technical guidelines or standards for achieving the same. No standards have been offered for the security of password, functionality, utilization of PKI for verification, virus scans, utilization of complex passwords, and management of account credentials. It doesn't offer guidelines for social engineering or spear phishing.
- Legal guiding principles have been given at several places in the government framework; but, they all repeat the existing rules and laws which include IT Amendment Act 2008, IT Act and RTI Act. Though the majority of the issues are considered by these laws, however, social networking has developed possibilities for social crimes and technological behavior that may not be as such covered by these laws, so, existing IT related laws have to be continuously augmented in order to check the new criminal offenses.
- Relating to citizen conduct, guidelines have been depicting clearly how a governmental agency should sort comments and how they should be engaged with the citizens. They define when and who it's mandatory and not mandatory to respond to various comments. They also define how and why comments that have an impact on the policy decision making must be preserved.
- The guidelines are normally silent about data availability and integrity, information confidentiality, and procedures, government organizations should adopt this trio. Although the policy, in general, refers to the devotion of different sections of IT Act 2000 as well as its amendment. However, there is no direct reference given to information security standard or act. ICT confronts severe challenges of security but very limited or no specific guidelines are offered for information security training and education.
- The guidelines fail to address risk mitigation, risk management, and acceptance issue of residual risks by the utilization of social networking. Although the guidelines support organizations to perform service level agreements along with social media website's operators but they don't mention guidelines regarding what agencies ought to seek out from these particular operators with respect to stronger security plus privacy controls, cross-site scripting, multifactor authentication, content monitoring and moderation, persistent cookies, access to various employees official accounts, and code signing and validation.

The guideline doesn't give emphasis on the periodic awareness as well as training of best practices, security, policy, for social media. It doesn't instruct organizations to constantly and periodically update their policy especially according to privacy and security, acceptable use and content filtering.

IX. Recommendations for Various Improvements

The W20SWG (Web 2.0 Security Working Group) in charge of accessing issues of information security surrounding various Web 2.0 technologies in the USA Federal Government has offered recommendations and Guidelines for utilizing social networking technologies in such a manner which minimizes the different risks included in it [20]. The manuscript encourages the utilization of social media in different government organizations and it also encourages following security guidelines. The government recommendations contain 5 categories of controls organized into non-technical and technical controls. The non-technical controls are specialized training, acquisition controls, and policy controls and the technical controls include host and network controls. The security controls must be adequately personalized in order to make the integration of social networking in e-governance.

The particular policy document for the utilization of social media/networking in e-governance must incorporate guidelines to achieve availability, integrity, and confidentiality of data and information. It has to offer guidelines for the utilization of several measures of network security control including the usage of trusted Internet connection, intrusion prevention system, intrusion detection system, and different methods of website content filtering such as deep packet inspections and traffic filtering, security zone creation, multi-facet authentication, utilization of domain name security and various other emerging safety & security technologies. Clear guidelines should be incorporated for the purchase of different social media services and various service level agreements for the sake of enhanced privacy, security and monitoring controls. Apt risk assessment and residual risk acceptance must be made with the help of the third party prior to selecting the utilization of a social media service that should be reassessed sporadically. Including social media in e-governance particularly in developing countries for example, India should necessarily incorporate various standards for security training & the assessment of technical skills corresponding to the employee before giving access to social networking websites for

ISSN: 2278 – 1323

authorized or official purposes.

Different federal government organizations may need different access policy of employee and so a uniform access policy might not be suitable for all type of government organizations. For example, in a research or academic government functionary where workers are engaged in knowledge sharing and collaborative activities, personal development of employee plays an important role in the development of organization accessibility to certain social media websites. So, policy should be flexible enough to let agencies allow the utilization of social networking sites during the office working hours for their professional development. In this scenario improvement of the accountability system is desired which can be performed in the form of log maintenance of all sorts of online activities implemented during the office hours. The policy should incorporate strict guidelines for publicizing all of its social media accounts in order to control any confusion among its users. The work account should be utilized for only official purposes and work and must always remain the agency's property and should be always open for inspection and lastly surrendered on retirements or transfers. Policies of local and state government vary on the scale and they might differ as per the management of social networking accounts. The policy of acceptable use should set boundaries around personnel, professional, and agency utilization of the social networking tools. The existing standard conduct code followed in government organizations doesn't address issues of the employee online conduct particularly when employing tools of social media. So, a successful policy of social media should directly address various issues of employee conduct connected with the social media use. To prevent inconsistency between web page content on social media and other print and electronic media pages of the organization, the social media policy should contain precise penalties and strict rules for its violation. Particular guidelines need to design for e-content preparation and authentication; non-reputation and integrity of e-content and author's liability need to be defined.

X. CONCLUSION

Different advantages of social networking or social media such as collaboration, empowerment, and participation have attracted various governments to utilize social media in governance for uniting citizens, agencies, and agencies information and work. It is utilized to advertise e-services, improve governmental trust and increase transparency. Aggressive, pervasive and persistent threats are confronted by governmental information systems which get boosted with the help of the environment developed by social networking as it contains risks on different fronts incorporating those related to ergonomic configuration, behavior, technology and regulation. When utilized in e-governance, social networking or social media might also pose various risks of exclusion, isolation, privacy violation, and information misuse and security threats. So, governments have developed comprehensive frameworks, best practices, guidelines, and policies to work as a key enabler for federal government agencies for the utilization of social media in e-governess. Various policies focus on different elements and the majority of them indicate the adherence of existing rules and regulations for securing information and data. The framework of Indian government is in tune with various other policies and it also incorporates policy for its multilingual cultural. But, it doesn't include guidelines for all determined core elements or doesn't give sufficient guidelines to few of the parameters that a social media policy must have. There is an extent or scope of improvement in every element incorporated in this government framework particularly in the guidelines corresponding to security controls, risk assessment, third party services acquisition, risk assessment, account management, and employees training.

REFERENCES

[1] Human Capital Institute, "Social Networking in Government: Opportunities and Challenges," January 2010.
[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, pp. 55-71, 2010.
[3] United Nations, "e-Government Survey," 2012.
[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, pp. 1-22, 2002.
[6] W. Darrell, "US State and Federal e-Government Full Report," 2002.
[7] N. Sampson, "Bank Marketing International: Simplifying in Formation," 2002.
[8] A. Kurunananda and V. Weerakkody, "e-Government Implementation in Sri Lanka: Lessons from the UK," Proceedings of 8th International Information Technology Conference, Colombo, pp. 53-65, 12-13 October 2006.
[9] F. Bélanger and L. Carter, "The Effects of the Digital Divide on e-Government: An Empirical Evaluation," Proceedings of the 39th Hawaii International Conference on System Sciences, Vol. 4, pp. 1-7, 2006.
[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, pp. 35-59, 2002.
[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 Ad-ministration Research and Theory, 2010.
[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, pp. 99-132, 2008-2009.
[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, pp. 371-391, 2005.
[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.
[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
[16] J. Michael Magro, "A Review of Social Media Use in e-Government," Administrative Science, Vol. 2, No. 2, pp. 148-161, 2012.
[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.
[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, pp. 135-147, 2010.
[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, pp. 1-19, 2009.
[21] P. Trudel, "Web 2.0 Regulation: A Risk Management Process," Canadian Journal of Law and Technology, Vol. 7, No. 2, pp. 243-265, 2010.
[22] DEIT, "Framework & Guidelines for Use of Social Media for Government Organizations," Department of Electronics and Information Technology, Government of India, 2012.

ISSN: 2278 – 1323

 **Ramandeep Kaur** received her M.Tech degree in computer science and engineering from Punjabi University, Patiala. Her research interest includes Digital Image Processing, Computer Graphics, and Image Forensics.

 **Dipen Saini** received his M.Tech degree in computer science and engineering from Guru Nanak Dev University, Amritsar. His research interest includes Digital Image Processing, Neural Networks, Natural Language Processing, and Machine Learning.

ISSN: 2278 – 1323