Evaluating Australian Social Media Policies in relation to the issue of Information Disclosure

Dinithi Pallegedara
School of Information and Business Analytics
Deakin University
Melbourne, Australia
Email: dpallege@deakin.edu.au

Matthew Warren
School of Information and Business Analytics
Deakin University
Melbourne, Australia
Email: matthew.warren@deakin.edu.au

Abstract

Information disclosure is a key concern for many organisations especially in the era of social media. Social media allows for information disclosure to occur easily due to the ubiquitous usage of technology such as mobile devices. Acceptable social media policies can be used by organisations and their employees to improve their decision making behaviours as well as being used as a controlling mechanism to mitigate the issue of information disclosure. Through a review of related research literature along with a content analysis of publicly available Australian social media policies, this paper identifies a perceived gap pertaining to the issue of information disclosure in current Australian social media use policies. To fill this gap, we have highlighted the key components when developing an organisational social media policy. An evaluation criteria is also proposed by the paper that organisations can use to assist in mitigating the information disclosure.

Keywords

Information disclosure, social media, social media policy, evaluation criteria, information security.

INTRODUCTION

Social media employs mobile and web-based technologies to create highly interactive platforms which individuals and communities share information, collaborate, discuss, facilitate and modify one or more media rich functionalities (Kaplan and Haenlein 2010; Kietzmann et al. 2011 p. 241; Senadheera et al. 2011). With the emerging developments in Web 2.0 applications like social media, organisations have adapted this technology to improve their internal operations as well as to interact with customers, business partners and suppliers (Culnan et al. 2010). When social media is used properly, it can offer a wide range of business advantages for both private and government organisations such as improving competitive advantage, brand awareness, customer relationships, online support, networking and information sharing. Conversely, there are a lot of risks and challenges in terms of associating social media usage by employees.

Recent media reports have revealed that some organisations face incidents where employees inadvertently disclose confidential information on social networking sites. The chief technologist and interim vice president of engineering for HP's cloud services business, accidently posted the 2011 strategic plans for HP's cloud computing, networking and storage services, shared management services on his LinkedIn page in advance of the company's official news release. This caused damage to the company's reputation and could have given advantages to their competitors (Braga 2011). A social media status update could contain a company secret or information about an upcoming launch and these accidental disclosures by employees could potentially cause havoc to the entire organisation. If the shared information is seen by an ordinary person who has no interest in this regard, there is no harm but when it comes to a potential competitor of the company, then there is a potential issue to consider. A careless or accidental use of social media could cause a wide range of negative impacts to an organisation in terms of reputational harm, financial and productivity loss, erosion of competitive advantage, potential lawsuits, legal penalties and malware risks (Colwill 2009; Gudaitis 2010; Young 2010).

Disclosure of organisational information can occur when information such as client confidential details, competitively sensitive knowledge, corporate strategies, internal policies, production processes and profitability are disclosed without permission to unauthorised parties (Anand and Rosen 2008). Disclosures can occur deliberately by a disgruntled employee or inadvertently due to human error but the latter is potentially regarded

as difficult to control (Hoecht and Trott 2006). Disclosures not only occur in social media but also through the use of other technologies and traditional forms of communication such as face-to-face conversations, documents, files, servers, printing facilities (Ahmad et al. 2005; CISCO 2008; Molok et al. 2011). However, social media is the most powerful channel of disclosure when considered with other forms of communication channels due to a larger potential social media audience. A conversation posted on social media could become available in the public domain, indexed by Google and archived for some time or permanently accessible in a virtual space via a search engine (Gudaitis 2010; Schneier 2009). Hence, the ubiquitous nature of social media could make it difficult for users to draw a true boundary between their work and personal life and that leads them to share personal and business information with a trusting attitude (Colwill 2009). As a result, organisations are becoming increasingly concerned about the disclosure (accidental or deliberate) of information through social media (Gaudin 2009; Wilson 2009).

When considering social media as an emerging technology, Schein (2010) believes that organisations could gain more benefits by implementing flexible social media policies which consider the nature of the technology and the employees' behaviours; and through the creation of shared norms, meanings and assumptions that comprise organisational culture. To date, little research has been done in the context of organisational social media policy evaluation and there is a lack of understanding within organisations concerning how to develop a good social media policy. Although, some organisations do have a social media policy in place, the issue of information disclosure, risks and mitigation approaches have not been given much attention in these policies. This is the main issue identified in this research. Hence, the authors believe that implementing acceptable social media use policies is the foundation for controlling inadvertent disclosure through social media in a corporate environment.

This research in progress paper is motivated by an observed gap in the literature of social media policy development and the issue of information disclosure. This paper aims to contribute to effective social media policy development by proposing an evaluation criteria and a rating tool in order to assess and improve social media policies effectiveness in organisations. The issue of information disclosure, security, target audience and technology aspects are addressed in our evaluation criteria which are not previously addressed in other forms of existing evaluation criteria. The next section describes a review of the related literature and the proposed evaluation criteria. We present results of a content analysis of twenty Australia social media policies in order to identify the gaps in the current organisation social media policies and the empirical analysis of the information disclosure practices in the Australian context. Finally, the conclusion highlights the contributions of the paper and areas for future research.

A REVIEW OF SOCIAL MEDIA POLICY LITERATURE

Organisations both large and small, government or private agencies have mechanisms to control the problem of information disclosure in the form of technical controls, information security policies, security education, training and awareness (Molok et al. 2010). Information systems literature emphasises the advantage of information security policy and practices, awareness training and strategies as a possible solution to mitigate disclosure. Many academic researchers recommend that the awareness of information leakage and its routes could mitigate the issue of information disclosure (Straub et al. 2004; Workman and Gathegi 2007). Information systems security management literature proposes that policy development is an effective controlling mechanism compared to technical and legal control mechanisms (Bulgurcu et al. 2010; Theoharidou et al. 2005; Workman and Gathegi 2007).

Organisations develop various types of policies to sufficiently address the organisational requirements for employees (Howlett 2009; Moule and Giavara 1995). Mainly there are two types of policies commonly used such as public policies and private policies (Hale 1988; Moule and Giavara 1995). Public policies are used within government departments to signify actions in order to obtain certain results whereas private policies are used by non-government organisations (Althaus et al. 2008). Since the organisations mostly depend on a wide variety of technologies in the modern world, policies have become more comprehensive because the policy has to cover every aspect of operational and strategic level activities (Doherty et al 2010). Therefore, the comprehensiveness has led to the development of different policies within an organisation to specify guidelines for different areas such as communication specific or technology specific policies.

Proliferation of social media has signified the need for the development of social media technology-specific policies in organisations. In general, policy development lacks guidelines for social media and in most cases, social media policies are tend to be comprehensive in nature. However, organisations could benefit by implementing flexible social media policies considering the nature of the technology and the employees' behaviours (Husin and Hanisch 2011a). Although there is a growing interest in the development of social media policies, relatively few sets of criteria have been proposed for assessing social media policies. A review of the academic and practitioners' literature revealed some of the evaluating criteria in developing social media policies in organisations (Doherty et al. 2011; Flynn and Kahn 2003; Hrdinová et al. 2010; Husin and Hanisch 2011a;

Husin and Hanisch 2011b; Kruger et al. 2013). Although these methods have been developed to assist organisations to improve the effectiveness of policy development, they have failed to address the issue of information disclosure occurs via the channel of social media. Hence, it is necessary to identify the important components of a social media policy in regards to the issue of information disclosure.

There are certain ways that organisations try to manage employee access using social media. Many organisations restrict access to the Internet for non-work related purposes such as social media. Therefore, it is necessary to mention the organisation's status so that it is easier for the employees to understand the overall position of social media in their organisation (Hrdinová et al. 2010; Husin and Hanisch 2011a; Husin and Hanisch 2011b; Kruger et al. 2013; Scott and Jacka 2011). Flynn and Kahn (2003) emphasise that the issue of who has the authority to post content on official organisational social media page and who is responsible for confirming and monitoring its accuracy is imperative. Generally, acceptable use policies encompass an organisation's position on how employees are expected to use organisation resources, their responsibilities, restrictions on use for personal interests and consequences for breaching the policies (Hrdinová et al. 2010; Husin and Hanisch 2011a; Kaganer and Vaast 2010; Kruger et al. 2013; Scott and Jacka 2011; Von Solms and Von Solms 2004). Simultaneously, a social media policy needs to be cross referenced and supported by other relevant policies, standards, country's legislations and regulations (Höne and Eloff 2002; Husin and Hanisch 2011b). According to Husin and Hanisch (2011a), training is regarded as compulsory to create awareness among the employees as well as to maintain standardisation in the policy document.

Flynn (2009) suggests that when developing policies for communication channels, it is necessary to provide rules in order to control the content to mitigate the risks to an organisation. For example, employees may inadvertently post personally identifiable or confidential information on social media which could negatively impact the organisation. This is a key concern that needs to be addressed in a social media policy (Flynn and Kahn 2003; Hrdinová et al. 2010; Husin and Hanisch 2011a; Husin and Hanisch 2011b; Kaganer and Vaast 2010; Scott and Jacka 2011). Some authors claim that a social media policy should be protected against the existing laws and regulations such as copyright, privacy and standard disclaimers for public records (Earp et al. 2002; Flynn and Kahn 2003; Grensing-Pophal 2010; Hrdinová et al. 2010; Husin and Hanisch 2011a; Kruger et al. 2013; Xu et al. 2010).

In an organisation, there are various stakeholders involve in numerous ways and therefore, addressing the guidelines to the relevant audience is vitally important to an effective social media strategy (Althaus et al. 2008; Husin and Hanisch 2011a; Husin and Hanisch 2011b; Kruger et al. 2013; Scott and Jacka 2011; Von Solms and Von Solms 2004). Another significant concern is that many social media policies often do not highlight the various devices that can be used to access social media channels, platforms and tools within each channel that will be used by the employees. It is regarded important because each platform is different in terms of the functionality and the purpose of use (Kaganer and Vaast 2010; Husin and Hanisch 2011a; Husin and Hanisch 2011b; Scott and Jacka 2011). Considering the critical components identified from the literature review, an evaluation criteria was thus generated as a method of developing effective social media policies in organisations. The components of the criteria are explained in the next section.

EVALUATION CRITERIA

In this study, we define the term "evaluation criteria" as an approach of evaluating the degree to which policies are able to meet objectives through comparison of their strengths and weaknesses. The evaluation criteria were developed as a framework to allow researchers, practitioners and professionals to develop effective social media policies for their organisations, especially in addressing the issue of organisational information disclosure. Policy makers could assess their current social media policies and identify what characteristics have not been addressed using the criteria in order to help organisations to develop or improve their social media policies. As shown in Table 1, the authors have developed the following six categories in reference to academic and practitioners' observations specifically drawing much attention to the issue of information disclosure. The components of the evaluation criteria were chosen based on their applicability and importance within a policy.

Table 1. The Evalutation Criteria

Evaluation component	Description	References
1. Officialdom	- Define the overall position or official status on social media use, - Establish boundaries on employee access for professional use, official use and personal use,	Flynn and Kahn 2003; Hrdinová et al. 2010; Husin and Hanisch 2011a; Husin and Hanisch 2011b;

	- Monitor social media activities of the employees, - Give permission to authorised employees to post content.	Kruger et al. 2013; Scott and Jacka 2011.
2. Acceptable use and consequences	- Define the employee conduct on how employees are expected to use organisation resources and their responsibilities, - The consequences of inappropriate conduct, - Cross reference with other relevant policies. For example: the code of conduct, - Provide training to create awareness among the employees.	Höne and Eloff 2002; Hrdinová et al. 2010; Husin and Hanisch 2011a; Husin and Hanisch 2011b; Kaganer and Vaast 2010; Kruger et al. 2013; Scott and Jacka 2011; Von Solms and Von Solms 2004.
3. Information disclosure	- Define the inadvertent posting of personally identifiable or confidential information, - Provide relevant guidelines to control the content to mitigate the risks of information disclosure.	Flynn and Kahn 2003; Flynn 2009; Hrdinová et al. 2010; Husin and Hanisch 2011a; Husin and Hanisch 2011b; Kaganer and Vaast 2010; Scott and Jacka, 2011.
4. Legal and privacy issues	- Define the existing laws and regulations, - Provide relevant privacy issues, - Use a standard disclaimer when engaging in social media activities.	Earp et al. 2002; Flynn and Kahn 2003; Grensing-Pophal 2010; Hrdinová et al. 2010; Husin and Hanisch 2011a; Kruger et al. 2013; Xu et al. 2010.
5. Target audience	- Define the related target audience, - Provide the expected level of engagement or responsibilities for the specific audience.	Althaus et al. 2008; Husin and Hanisch 2011a; Husin and Hanisch 2011b; Kruger et al. 2013; Scott and Jacka 2011; Von Solms and Von Solms 2004
6. Relevant use of technology channel	- Define the detailed guidelines on how to access different social media channels, platforms and tools such as Facebook, Twitter, LinkedIn, YouTube, Yammer & Intranet, Blogs & Personal sites and Devices.	Kaganer and Vaast 2010; Husin and Hanisch 2011a; Husin and Hanisch 2011b; Scott and Jacka 2011.

The evaluation criteria were used to analyse the effectiveness of twenty publicly available Australian social media policies. In this study the content analysis method was used to evaluate the qualitative aspects of the social media policies. As for this study, the samples were chosen randomly and the four sample groups were selected. These were Australian Federal Government, Australian State Government, Australian Universities and Australian Stock Exchange (Top 100 companies). The reason for choosing these four different samples was to explore the variation of social media policies for different industry sectors. For each of this sample, five organisations were chosen at random and the social media policy documents were obtained from the organisational website. The following section presents the results of the content analysis and criteria evaluation. We have applied a basic 6 points rating system to rank each component within the policies. Each component is given a maximum of 1 point depending on the level of information supplied and the relevancy in the policy. For example, Officialdom is consisted of four elements. If the policy has addressed all the four elements, then the awarded grade is equivalent to 1 point. If a policy has addressed only three elements, then the awarded grade is 0.75. If the overall grade is higher than 4 points, it can be considered as a policy with a satisfactory coverage.

RESEARCH RESULTS

Australian Federal Government Social Media Policy Analysis

Out of the five federal government social media policies (see Table 2), the majority of the documents clarified the degree of official, professional and personal usage of social media by the employees. The Department of Finance and Deregulation allows personal use of social media only for incidental to formal duties whereas the Department of Agriculture, Fisheries and Forestry approves only the social media channels that do not pose a technical threat to the organisation. Hence, access to audio and video sharing websites are restricted. Further they have emphasised that staff must not use their official departmental account, email address or other departmental title, contact details for any unofficial use. As long as the staff member does not make any reference to the Australian National Botanical Gardens, the policy does not apply to its employees. Most of the federal government departments in the sample monitor the access to social media channels for reasonable use except for the National Library of Australia. Only the Department of Finance and Deregulation has considered the relevant technology channel with proper guidelines on how to use each platform. Information disclosure is only partially explained including the types of information that cannot be disclosed to the public in the social media policy of the Department of Finance and Deregulation. Although the five policies in the sample emphasise that the employees should not reveal confidential information, the guidelines need to be expanded.

Table 2. Evalutation of the Australian Federal Government Social Media Policies

Organisation	Officialdom (1)	Acceptable use (1)	Information disclosure (1)	Legal & privacy (1)	Target audience (1)	Technology channel (1)	Rate (1-6)
Dept. of Human Services *Date effective: 2013*	Official status, Establishing boundaries, Monitoring, Permission	Employee conduct, Consequences, References, Training	Confidentiality, Guidelines	Disclaimer, Legal, Privacy	Applicability, Responsibilities	None	4
Dept. of Finance and Deregulation *Date effective: 2012*	Official status, Establishing boundaries, Monitoring, Permission	References	Confidentiality, Guidelines	Disclaimer, Privacy	None	Facebook, Twitter	3.75
Australian National Botanic Gardens *Date effective: 2010*	Official status, Establishing boundaries, Monitoring, Permission	Employee conduct, References, Training	Confidentiality	Disclaimer, Privacy	Applicability	None	3.75
National Library of Australia *Date effective: 2012*	Official status, Establishing boundaries, Permission	Employee conduct, Consequences, References	Confidentiality, Guidelines	Disclaimer, Legal, Privacy	Applicability	None	4
Dept. of Agriculture, Fisheries and Forestry *Date effective: 2012*	Official status, Establishing boundaries, Monitoring, Permission	Employee conduct, References	Confidentiality, Guidelines	Disclaimer, Legal, Privacy	Applicability, Responsibilities	None	4.5

Australian State Government Social Media Policy Analysis

The state government social media policies have covered the aspects of how to differentiate the official and personal usage of social media (see Table 3). The New South Wales (NSW) Police Force has two different social media policy documents for official and personal usage. However, the Victoria (Vic) Department of Health's guidelines do not apply to staff members' personal use of social media platforms where they make no reference to the Victorian Government, the Department of Health, its staff, policies and services, business partners, suppliers or other stakeholders. Also, it denotes that public servants can write and contribute to personal social media in their own time using their own resources. The relevant use of technology channel is not discussed properly in any of the policies except for the NSW Police Force and the Department of Human Services in Victoria where the policies have given details on how to use Facebook, Twitter, LinkedIn, Intranet and other personal devices. The Vic Department of Health has provided separate guidelines for different staff members who participate in social media. The majority of the policies have specified the importance of keeping confidential information safely but the ways on how to deal with the issue is lacking. NSW Police Force has provided examples on how information disclosure can happen deliberately or inadvertently and that seems to be a better procedure in highlighting this issue to the social media users.

Table 3. Evalutation of the Australian State Government Social Media Policies

Organisation	Officialdom (1)	Acceptable use (1)	Information disclosure (1)	Legal & privacy (1)	Target audience (1)	Technology channel (1)	Rate (1-6)
NSW Police Force *Date effective: 2011*	Official status, Establishing boundaries, Monitoring, Permission	Employee conduct, Consequences, References	Confidentiality, Guidelines	Disclaimer, Legal, Privacy	Responsibilities	Facebook, LinkedIn, Devices	4.25
NSW Government *Date effective: No Date*	Official status, Establishing boundaries	Employee conduct, References	Confidentiality, Guidelines	Disclaimer, Legal, Privacy	Applicability	None	3.5
VIC Dept. of Health *Date effective: 2010*	Official status, Establishing boundaries, Permission	Employee conduct, References, Training	Confidentiality, Guidelines	Disclaimer, Privacy	Applicability, Responsibilities	None	3.83
VIC Dept. of Justice *Date effective: 2011*	Establishing boundaries	Consequences, References	None	None	Applicability	None	1.25
VIC Dept. of Human Services *Date effective: 2011*	Official status, Establishing boundaries, Permission	Employee conduct, Consequences, References	Confidentiality, Guidelines	Disclaimer, Legal, Privacy	Applicability	Facebook, Twitter, Yammer & Intranet	5

Australian Universities Social Media Policy Analysis

The majority of the university social media policies have established a boundary between personal and official use of social media (see Table 4). In most cases, the policy is not applicable for personal use of social media channels as long as the staff makes no reference to university matters. Compared to other policies, Monash University has few social media policies applicable for different set of users. However, the policy is applicable for personal purposes where a staff member can be identified as a Monash employee only. In contrast, University of Western Australia's policy mainly focuses on clarifying boundaries for private identity. The Monash University social media policy has mentioned the fact that it covers the use of social media by any means such as computer, tablet, mobile phone or any handheld device. All the five universities in the sample have discussed the importance of maintaining sensitive and confidential university information. Nevertheless, the guidance provided on how to mitigate information disclosure through social media is lacking. The University of Newcastle and the University of Melbourne have given instructions on how to use different social media platforms such as Facebook and Twitter.

Table 4. Evalutation of the Australian Universities Social Media Policies

Organisation	Officialdom (1)	Acceptable use (1)	Information disclosure (1)	Legal & privacy (1)	Target audience (1)	Technology channel (1)	Rate (1-6)
Deakin University *Date effective: No Date*	Official status, Establishing boundaries, Permission	Employee conduct, Consequences, References, Training	Confidentiality, Guidelines	Disclaimer, Legal, Privacy	Applicability	Blogs	4.5
University of Newcastle *Date effective: 2011*	Official status, Establishing boundaries	Employee conduct, Consequences, References, Training	Confidentiality, Guidelines	Disclaimer	None	Facebook, Twitter, YouTube, Blogs	3.83
University of Melbourne *Date effective: 2010*	Official status, Establishing boundaries, Permission	Employee conduct, References	Confidentiality, Guidelines	Disclaimer, Privacy	Applicability	Facebook, Twitter	3.91
Monash University *Date effective: 2013*	Official status, Establishing boundaries, Permission	Employee conduct, Consequences, References	Confidentiality, Guidelines	Disclaimer, Legal, Privacy	Applicability , Responsibilities	Devices	4.75
University of Western Australia *Date effective: 2011*	Official status, Establishing boundaries	Employee conduct, Consequences, References	Confidentiality, Guidelines	Disclaimer, Legal, Privacy	None	None	3.25

Australian Stock Exchange 100 (ASX100) Social Media Policy Analysis

Out of the five company examples of ASX100 (see Table 5), JB Hi-Fi and Coca Cola Amatil did not explicitly set the boundaries for official, professional and personal use of social media. The Telstra policy applies for personal use only if a person is discussing Telstra or Telstra related issue in his/her personal use of social media. Conversely, the NAB social media policy is mainly focused on personal use. On the other hand, JB Hi-Fi policy does not allow the use of social networking during work hours. The target audience and the relevant use of

technology channel are not presented in these policies. Information disclosure is hardly mentioned by any of the guidelines. However, Telstra and NAB policies have given examples of the types of confidential information that cannot be disclosed to the public.

Table 5. Evalutation of the ASX100 Social Media Policies

Organisation	Officialdom (1)	Acceptable use (1)	Information disclosure (1)	Legal & privacy (1)	Target audience (1)	Technology channel (1)	Rate (1-6)
Telstra *Date effective: No Date*	Official status, Establishing boundaries, Permission	Employee conduct, Consequences, References, Training	Confidentiality, Guidelines	Disclaimer, Legal, Privacy	Applicability	None	4.25
NAB *Date effective: 2011*	Official status, Establishing boundaries	Employee conduct, References	Confidentiality, Guidelines	Disclaimer, Legal, Privacy	None	None	3
Suncorp *Date effective: 2011*	Official status, Establishing boundaries	Employee conduct, Consequences	Confidentiality	None	None	None	1.5
JB Hi-Fi *Date effective: 2012*	Official status, Permission	Employee conduct, Consequences, References	Confidentiality, Guidelines	Legal, Privacy	None	None	2.91
Coca Cola Amatil *Date effective: 2012*	Official status, Permission	Employee conduct, Consequences, References	Confidentiality, Guidelines	Disclaimer, Legal, Privacy	Applicability	None	3.75

SUMMARY OF THE EVALUATION

Overall, the Department of Human Services in Victoria has received the highest rate among the social media policies while receiving 5 points with a satisfactory coverage of most of the aspects that we have identified followed by the Monash University with 4.75 points, the Department of Agriculture, Fisheries and Forestry with 4.5 points and the Deakin University with 4.5 points. In contrast, Department of Justice in Victoria received the lowest score of 1.25 points.

From the analysis, it is evident that most of the organisations in the sample address the components for officialdom, acceptable use and consequences, legal and privacy issues. A number of organisations have differentiated the boundaries between personal, professional and official use of social media. NSW Police Force is the only organisation with two separate policy documents for staff's personal and official use of social media. Some organisations state that the staff should use their real name and identify themselves as staff members when using social media in a personal capacity whereas others state that staff must not use their official departmental account, email address or other departmental details for any unofficial use. One of the key observations in the social media policy analysis is that the policy applies only if a person mentions the organisation's name or makes references to related issues of the organisation in his/her personal use of social media.

Target audience and the relevant use of technology channel are the least addressed aspects in the social media policies in the sample. The Monash University has three social media policy documents for different audiences. Some of the social media policies have given specific guidelines for different stakeholders. Only the NSW Police Force and the Monash University have covered the use of social media by any means including computers, tablets, mobile phones or handheld devices. The issue of information disclosure which is the main focus on this study has not been addressed properly in any of the social media policies except for the NSW Police Force. The NSW Police Force has given examples on topics where information disclosure can happen inadvertently or deliberately. Most of the other policies have mentioned that employees must not comment on or disclose information but do not provide proper guidance on how to mitigate the disclosure of information. As a whole, there is a gap in the social media policies in relation to the issue of information disclosure.

CONCLUSION AND FUTURE RESEARCH

The emergence of social media usage in organisations and the increased demand of technology devices have indicated the need for sophisticated social media policies to be implemented by the management to provide guidelines for both the organisation and its employees. Policy makers have recognised the need for improved social media policies to protect confidential and sensitive information being disclosed to unauthorised parties by employees. Findings from this research indicate that traditional policy development components are not appropriate for social media policy development pertaining to the issue of information disclosure. Despite the fact that there are social media policies in place, our empirical analysis provides evidence that the majority of the policies from four different sectors in Australia do not satisfactorily address the necessary components to assist organisations in social media policy development. We emphasise the need for understanding the risk associated

in the organisational information disclosure and the need to address this global phenomena appropriately in social media policies. Although social media policy development has been increasing in organisations, relatively few sets of criteria have been proposed for evaluating social media policies. Our proposed evaluation criteria can be adapted as a guiding tool to enhance social media policies, specifically to address the issue of information disclosure.

Furthermore, considering the rapid changes occur in social media technologies, it is necessary to update the social media policies as an ongoing process. Hence, the analysis of the social media policies have to be evaluated from time to time in order to observe the effectiveness because during the time this analysis was conducted, there have been many changes and alterations even in the policies that we primarily analysed. Also, there will be more components that can be applied to the evaluation criteria. Therefore, our criteria is a preliminary investigation and an ongoing research to test the criteria in practice. Hence, as a next step, we aim to develop a framework towards assisting organisations to develop social media policies by addressing the issue of information disclosure considering the significant components identified in this preliminary analysis. Further research is needed in order to provide more comprehensive guidelines in social media policy development in controlling the information disclosure.

REFERENCES

Ahmad, A., Ruighaver, A. B., and Teo, W. T. 2005. "An Information-Centric Approach to Data Security in Organizations," TENCON 2005 IEEE Region 102005, pp 1-5.

Althaus, C., Bridgman, P., and Davis, G. 2008. *The Australian Policy Handbook 4*, (5 ed.) Allen & Unwin: Australia.

Anand, V., and Rosen, C. 2008. "The ethics of organizational secrets," *Journal of Management Inquiry* (17:2), pp 97-101.

Australian Government, Australian National Botanic Gardens. 2010. Social Media Policy. [Online]. Retrieved 10 September 2013, from http://www.anbg.gov.au/gardens/about/management/policy-docs/social-media-policy-10-03-24.pdf.

Australian Government, Department of Agriculture. 2012. Social Media Policy. [Online]. Retrieved 9 September 2013, from http://www.daff.gov.au/about/social-media/policy.

Australian Government, Department of Finance and Deregulation. 2012. Social Media 101: A beginner's guide for Finance employees. [Online]. Retrieved 12 September 2013, from http://www.finance.gov.au/files/2010/04/social-media-101.pdf.

Australian Government, Department of Human Services. 2013. Social Media Policy. [Online]. Retrieved 10 May 2014, from http://www.humanservices.gov.au/spw/corporate/site-information/resources/8348-1212-social-media.pdf.

Braga, M. 2011. "Can't stop the tweet: the peril—and promise—of social networking for IT," arstechnica. [Online]. Retrieved 03 March 2013, from http://arstechnica.com/business/2011/10/cant-stop-the-tweet-the-periland-promiseof-social-networking-for-it/.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," *MIS quarterly* (34:3), pp 523-548.

CISCO 2008. "Data Leakage Worldwide: Common Risks and Mistakes Employees Make," Cisco Systems Inc, San Jose, CA.

Coca Cola Amatil. 2012. Code of Business Conduct – Acting with Integrity. [Online]. Retrieved 15 October 2013, from http://ccamatil.com/AboutCCA/Corporate%20Governance/Codes%20and%20Policies/Code%20of%20Business%20Conduct%20Policy%20%287%20Nov%202012%29.pdf.

Colwill, C. 2009. "Human factors in information security: The insider threat – Who can you trust these days?," *Information Security Technical Report* (14:4), pp 186-196.

Culnan, M. J., McHugh, P. J., and Zubillaga, J. I. 2010. "How Large U.S. Companies Can Use Twitter And Other Social Media To Gain Business Value," *MIS Quarterly Executive Journal* (9:4), pp 243-259.

Deakin University. ND. Social Media Guidelines. [Online]. Retrieved 25 September 2013, from https://www.deakin.edu.au/socialmedia/assets/resources/deakin-social-media-guide.pdf.

Doherty, N. F., Anastasakis, L., and Fulford, H. 2011. "Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy," *International Journal of Information Management* (31:3) 6//, pp 201-209.

Earp, J. B., Antón, A. I., and Jarvinen, O. 2002. "A Social, Technical and Legal Framework for Privacy Management and Policies," *Americas Conference on Information Systems (AMCIS)*, pp. 605-612.

Flynn, N., and Kahn, R. E. 2003. *Email Rules: A Business Guide to Managing Policies, Security, and Legal Issues for Email and Digital Communication*, American Management Association: New York.

Flynn, N. 2009. *The E-Policy Handbook: Rules and Best Practices to Safely Manage Your Company's E-Mail, Blogs, Social Networking, and Other Electronic Communication Tools* AMACOM Div American Mgmt Assn.

Gaudin, S. 2009. "Study: 54 percent of companies ban Facebook, Twitter at work.," W. Blogs (ed.), Computerworld. [Online]. Retrieved 12 September 2012, from http://www.wired.com/business/2009/10/study-54-of-companies-ban-facebook-twitter-at-work/.

Grensing-Pophal, L. 2010. "The New Social Media Guidelines " *Information Today* (27:3), pp 1-47.

Gudaitis, T. 2010. "The Impact of Social Media on Corporate Security: What Every Company Needs to Know," Cyveillance, Inc: Virginia.

Hale, D. 1988. "Just What is a Policy, Anyway? And Who's Supposed to Make it? A Survey of the Public Administration and Policy Texts," *Administration & Society* (19:4), pp 423-452.

Hoecht, A., and Trott, P. 2006. "Outsourcing, information leakage and the risk of losing technology-based competencies," *European business review* (18:5), pp 395-412.

Höne, K., and Eloff, J. H. P. 2002. "Information Security Policy — What Do International Information Security Standards Say?," *Computers & Security* (21:5), pp 402-409.

Howlett, M. 2009. "Governance modes, policy regimes and operational plans: A multi-level nested model of policy instrument choice and policy design," *Policy Sciences* (42:1), pp 73-89.

Hrdinová, J., Helbig, N., and Peters, C. S. 2010. *Designing Social Media Policy for Government: Eight Essential Elements*. Center for Technology in Government, University at Albany.

Husin, M., and Hanisch, J. 2011a. "Social Media and Organisation Policy (Someop): Finding the Perfect Balance," *European Conference on Information Systems* Association for Information Systems.

Husin, M., and Hanisch, J. 2011b. "Utilising the Social Media and Organisation Policy (SOMEOP)," European Conference on Information Systems.

JB Hi-Fi. 2012. Code of Conduct. [Online]. Retrieved 13 October 2013, from https://www.jbhifi.com.au/Documents/Governance/code-conduct-29_2012-07-26_12-12-46.pdf.

Kaganer, E., and Vaast, E. 2010. "Responding to the (Almost) Unknown: Social Representations and Corporate Policies of Social Media," in: *Thirty First International Conference on Information Systems*. St. Louis.

Kaplan, A. M., and Haenlein, M. 2010. "Users of the world, unite! The challenges and opportunities of Social Media," *Business Horizons* (53:1), pp 59-68.

Kietzmann, J. H., Hermkens, K., McCarthy, I. P., and Silvestre, B. S. 2011. "Social Media? Get Serious! Understanding the Functional Building Blocks of Social Media," *Business Horizons Journal* (54:3), pp 241-251.

Kruger, N., Brockmann, T., and Stieglitz, S. 2013. "A Framework for Enterprise Social Media Guidelines," *Proceedings of the Nineteenth Americas Conference on Information Systems*, Chicago, Illinois.

Molok, N. N., Chang, S., and Ahmad, A. 2010. "Information Leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats," in *8th Australian Information Security Management*: Edith Cowan University, Perth Western Australia.

Molok, N. N., Ahmad, A., and Chang, S. 2011. "Exploring The Use of Online Social Neworking By Employees: Looking At The Potential For Information Leakage," in *15th Pacific Asia Conference on Information Systems*, Queensland University of Technology, pp 138.

Monash University. 2012. Conduct and Compliance Procedure – Staff Use of Social Media. [Online]. Retrieved 29 September 2013, from http://www.adm.monash.edu.au/workplace-policy/conduct-compliance/use-of-socialmedia.html.

Monash University. 2013b. Social Media: Student Use Procedures. [Online]. Retrieved 20 September 2013, from http://policy.monash.edu.au/policy-bank/management/global-engagement/social-media-student-use-procedures.html.

Monash University. 2013a. Social Media: Staff and Associates Use Procedures. [Online]. Retrieved 20 September 2013, from http://policy.monash.edu.au/policy-bank/management/global-engagement/social-media-staff-associates-use-procedures.html.

Moule, B., and Giavara, L. 1995. "Policies, procedures and standards: an approach for implementation," *Information Management & Computer Security* (3:3), pp 7-16.

NAB. 2011. Social Media Guidelines – How to present yourself online. [Online]. Retrieved 27 September 2013, from http://www.nab.com.au/wps/wcm/connect/a6ab800045b20e6cab5eef654f3deb8a/NDS0132_SocialMediaStaffGuidelines_A4.pdf?MOD=AJPERES.

National Library of Australia. 2012. Social Media Policy. [Online]. Retrieved 15 September 2013, from https://www.nla.gov.au/policy-and-planning/social-media.

NSW Government. ND. Social Media Policy. [Online]. Retrieved 15 September 2013, from http://www.advertising.nsw.gov.au/strategic-communications/social-media-policy.

NSW Police Force. 2011. Personal Use of Social Media Policy. [Online]. Retrieved 15 September 2013, from https://www.police.nsw.gov.au/__data/assets/pdf_file/0007/208609/personal-use-of-social-media-policy-and-guidelines.pdf.

NSW Police Force. 2013. Official Use of Social Media Policy. [Online]. Retrieved 15 September 2013, from http://www.police.nsw.gov.au/__data/assets/file/0010/261874/Official_Use_of_Social_Media_Policy.pdf.

Schein, E. H. 2010. *Organizational culture and leadership*, John Wiley & Sons.

Schneier, B. 2009. "Special Report: Industry experts debate social networking risks ", Security Asia. [Online]. Retrieved 08 August 2013, from http://security.networksasia.net/content/special-report-industry-experts-debate-social-networking-risks.

Scott, P. R., and Jacka, J. M. 2011. *Auditing Social Media: A Governance and Risk Guide*. John Wiley & Sons.

Senadheera, V., Warren, M., and Leitch, S. 2011. "A Study into How Australian Banks Use Social Media " in: *Pacific Asia Conference on Information Systems (15th : 2011 : Brisbane, Queensland)*. Brisbane, Qld., pp 12.

Straub, D., Rai, A., and Klein, R. 2004. "Measuring firm performance at the network level: A nomology of the business impact of digital supply networks," *Journal of Management Information Systems* (21:1), pp 83-114.

Suncorp. 2011. Code of Conduct. [Online]. Retrieved 01 October 2013, from http://www.suncorpgroup.com.au/sites/default/files/fm/documents/governance-documents/4.01%20Code%20of%20Conduct.pdf.

Telstra. ND. Telstra's 3 Rs of Social Media Engagement. [Online]. Retrieved 25 September 2013, from http://exchange.telstra.com.au/wp-content/uploads/2012/09/telstra-3rs-policy-2012.pdf.

Theoharidou, M., Kokolakis, S., Karyda, M., and Kiountouzis, E. 2005. "The insider threat to information systems and the effectiveness of ISO17799," *Computers & Security* (24:6), pp 472-484.

University of Melbourne. 2010. University of Melbourne's Social Media Guidelines. [Online]. Retrieved 23 September 2013, from http://www.marketing.unimelb.edu.au/social-media/social-media-guidelines.html.

University of Newcastle.2011a. Social Media Communication Guideline. [Online]. Retrieved 22 September 2013, from http://www.newcastle.edu.au/policy/000955.html.

University of Newcastle. 2011b. Social Media Communication Policy. [Online]. Retrieved 22 September 2013, from http://www.newcastle.edu.au/policy/000953.html.

University of Newcastle. 2011c. Social Media Communication Procedure. [Online]. Retrieved 22 September 2013, from http://www.newcastle.edu.au/policy/000954.html.

University of Western Australia. 2011. University Policy on: Social Media. [Online]. Retrieved 21 September 2013, from http://www.governance.uwa.edu.au/procedures/policies/policies-and-procedures?method=document&id=UP11%2F22.

VIC Government, Department of Justice. 2011. Social media policy. [Online]. Retrieved 15 September 2013, from http://www.justice.vic.gov.au/utility/social+media/social+media+policy.

VIC Government, Department of Health. 2010. Social Media Action Plan – Part 1: Policy. [Online]. Retrieved 16 September 2013, from http://www.egov.vic.gov.au/website-practice/web-2-0/social-networks-and-social-media-in-government/department-of-health-social-media-action-plan-part-1-policy.html.

VIC Government, Department of Human Services. 2011. Social media policy for employees. [Online]. Retrieved 17 September 2013, from http://www.dhs.vic.gov.au/__data/assets/pdf_file/0009/662976/DHSsocialmediapolicyforemployees_200911.pdf.

Von Solms, R., and von Solms, B. 2004. "From Policies to Culture," *Computers & Security* (23:4), pp 275-279.

Wilson, J. 2009. "Social networking: the business case - [IT internet]," *Engineering & Technology* (4:10), pp 54-56.

Workman, M., and Gathegi, J. 2007. "Punishment and ethics deterrents: A study of insider security contravention," *Journal of the American Society for Information Science and Technology* (58:2), pp 212-222.

Xu, H., Parks, R., Chu, C., and Zhang, X. 2010. "Information Disclosure and Online Social Networks: From the Case of Facebook News Feed Controversy to a Theoretical Understanding," *Americas Conference on Information Systems*, Lima, Peru.

Young, K. 2010. "Policies and procedures to manage employee Internet abuse," *Computers in Human Behavior* (26:6), pp 1467-1471.

COPYRIGHT