Literature Review

Concerns of trust and privacy within the social networking sites

Cy Messenger | Marketing Strategy | BSNS7370 | Unitec Auckland | March 2012

Table of Contents

Introduction

In today's internet driven society we have witnessed the rapid growth of social network sites' (SNS) as well as their integration into our everyday lives. SNS's such as Facebook (FB), Twitter, Linkdin, Myspace and Bebo, now represent a fundamental shift in the way that we communicate (Butler, McCann , & Thomas , N.D) in our personal and working lives. In December 2011 FB alone reported to have 845 million active monthly users (Facebook, N.D). With the sharing nature of SNS's and the sites' control of posted information, concerns have developed regarding trust and privacy issues within SNS's.

This report is a literature review of ten published journals and articles related to the topic of trust and privacy within the social media space, taken from a users perspective. We will begin by discussing the user's responsibilities concerning their own online content, and go on to talk about the inconsistency and confusion of SNS's privacy policies. We will then discuss the concept of user's data being seen as currency, and the use of user's private and personal information. Next we will discuss how privacy laws governing the internet space are out of touch with modern internet usage, and talk about the security risks involved with sharing personal information on SNS's.

We will finish this report by offering recommendations to Government's, SNS users and SNS owners as to ways in which the social media space can be made safer and more private for users. Essentially being that Governments need to update privacy policies concerning the online space, that SNS users must be aware of SNS's privacy policies and take some responsibility for the information that they choose to post online, and finally that SNS's have to take a more ethical and socially responsible approach to their use of user information.

1.0 Concept Definitions

Social Network Sites; web applications that facilitate online relationships between people (Hooper & Evans, 2010). SNS's are referred to by varying terms, the definition is universal.

Trust; a belief or expectation about the other (trusted) party, or as a willingness to rely on another party, coupled with a sense of vulnerability or risk if the trust is violated (Grabner-Krauter, 2009). This is a universally accepted concept of trust.

Privacy; a state in which one is not observed or disturbed by other people. The state of being free from public attention: a law to restrict e.g. newspapers' freedom to invade people's privacy (Oxford Dictionaries, 2012). This is a universally accepted concept of privacy.

Privacy Statement; is a form of contractual commitment on the part of the company receiving the information, and one of the primary means customers have to identify the values of an organisation (Hooper & Evans, 2010). This is a universally accepted definition.

2.0 Literature Review

Individuals are no longer just consumers of online information. They now play a significant role in creating content for others to consume (Bateman, Butler, & Pike, 2010). The question is "*do SNS users hold the ultimate responsibility for their own content*?" It is contributed voluntarily after all. SNS's and the internet as a whole are public spaces, used to connect people. Gone are the days of regular communications being performed via written letters in sealed envelopes, however truly private and secure mail is still conducted this way through the likes of registered mail. Further questions are, "Can social network sites really be considered private?" ''What is private? Certainly not anything you put on the internet, no matter how many privacy controls there are" (Emerald, 2011). User's essentially trust that information posted to SNS's will be respected as being personal and private, only available for viewing by the intended limited audience.

A common (other) use of SNS's now is to allow employers to conduct informal background checks of prospective employees. This may sound unethical but there is no legislation or privacy policy to prevent this from occurring. What is to stop employers from making use of free and accessible resources to aid their decision-making? After all, the information has been put there by someone who is aware that it will be viewed and shared by others (Emerald, 2011). The issues arrive when posts are potentially being viewed by larger than intended audiences (Butler, McCann , & Thomas , N.D). Intended private information posted to SNS's being viewed and used for other purposes although questionable must ultimately be the responsibility of the user. The simple fact is that if a comment or image posted may someday lead to embarrassment or public scrutiny, then it should not be posted to this vast public space, regardless of any privacy policies that may be in place. Total privacy on SNS's simply is not possible (Hooper & Evans, 2010). However, SNS's are violating the trust of their users by making personal information available to larger than intended audiences.

Although all SNS's publish privacy policies, the SNS environment is largely devoid of security standards and practices (Grabner-Krauter, 2009). *Privacy statements are often inconsistent, confusing and incomplete* (Hooper & Evans, 2010), and appear to be more concerned with protecting the organisation than protecting user privacy and security (Hooper & Evans, 2010). While all SNS's offer similar services, policies and practices differ from site

to site. For example, FB's default settings do not tell users who views their information, while LinkedIn's default setting shows some details of who is viewing user information if it is accessed (Bateman, Butler, & Pike, 2010).

Every time the likes of FB introduce a new feature, user information seems to become more accessible, rather than less (Tan, Qin, Kim , & Hsu, 2011). Particularly with the introduction of 'Timeline' on FB where any posts made over the lifetime of a membership are viewable unless individually removed from the 'Timeline'.

Information posted to SNS's may also be used for other purposes; this is not always made clear to users by the SNS. FB founder Mark Zukerberg said, when commenting on this issue "People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time" (Tan, Qin, Kim , & Hsu, 2011). When users of a SNS use the site they are agreeing to the terms and conditions of that site. Therefore if a fraudulent activity of some sort occurs it can be argued that the fault is on the user due to the information being made public voluntarily, and the result of poor user awareness, having potentially not read or understood the privacy statement (Hooper & Evans, 2010). Younger users are more likely to share their personal information and are less likely to take the time to read privacy statements, suggesting that adult or older users are more concerned with privacy issues than younger users (Hugl, 2011).

The Internet has become a global medium for the gathering of personal information, generating data about users to assist in targeted marketing (Hooper & Evans, 2010). With millions of registered users visiting SNS's on a daily basis, the potential business value of user data has become too great to be ignored by today's marketers (Tan, Qin, Kim , & Hsu, 2011). *Information has become a form of currency*, exchanged by users in order to participate in the economy of social networking. Although many SNS's are free to use, users pay for the service with the information that they share (Bateman, Butler, & Pike, 2010). Personal details such as name, age, gender, likes, geographic location and favourite; music, movies, books and TV shows are sold to third parties. With this information marketers are able to target users with personalised advertising (Hugl, 2011). Data brokers also compile consumer information from both public and private sources and sell it to different organisations for a range of purposes including data mining, profiling and pre-recruiting information as well as for economic espionage (Hugl, 2011). SNS's unfortunate motivation for profit has been seen to overshadow their concerns for user privacy (Hooper & Evans, 2010).

As the SNS environment evolves over time so to must Government laws regarding privacy protection, as *many current privacy laws do not consider modern internet usage*. SNS's are governed for example in New Zealand by the Privacy Act 1993 (Hooper & Evans, 2010), in the USA by the Electronic Communications Privacy Act 1986 (US Legal INC, N.D), and in the UK by various acts dated 1998 to 2004, including the Privacy and Electronic Communications Regulations 2003 (Privacy, 2012). All of these privacy regulations were set before the rise of the SNS's. It has been argued that the US privacy regulations are not equipped to address SNS's (Hooper & Evans, 2010), as they do not specifically recognise privacy rights (McGrath, 2011). A website is therefore only required to honour it's own privacy policies, which are written to legally protect the website from any wrongdoing (McGrath, 2011). SNS users should not be dependent on SNS's to dictate how much privacy users will have. This is something that must be established in law (Sangani, 2010). When the law offers so little protection, it allows for the deliberate misuse of data without the need for consent. This situation is not helped by the global nature of the internet, with privacy protection varying in different jurisdictions (Hooper & Evans, 2010).

Using SNS's and *posting personal information both publically and privately can lead to a multitude of risks* including; identity theft, sexual exploitation, online stalking, and cyber harassment. Users may also be subjected to public scrutiny, possibly creating permanent records that may negatively affect the user in the future (Tan, Qin, Kim , & Hsu, 2011). The average user voluntarily provides information about their home address, pet's name, where he/she went to school, mother's maiden name and other family details. This is the typical information used for security or lost password questions for online services (Grabner-Krauter, 2009). You would expect that poor social network practices would only lead to outcomes that will negatively impact SNS's (Dinh, 2011). In recent years; Bebo admitted that a bug in its systems enabled users to view other users private information (Grabner-Krauter, 2009), Twitter agreed to a settlement with the US Federal Trade Commission over charges that it put users privacy at risk by failing to protect their personal information (Sangani, 2010) and FB users found their personal details exposed and searchable on Google, Bing and Yahoo (Sangani, 2010). Yet users keep using SNS's even after reports of privacy violations have been released (Tan, Qin, Kim , & Hsu, 2011).

SNS's would like to be seen as being law-abiding and socially responsible organisations, without being held legally responsible for any privacy breeches (Hooper & Evans, 2010). The SNS's therefore (through privacy statements) place full responsibility for consequences of site usage solely on the user (Hooper & Evans, 2010). This raises the question of "who owns user information once it is online and who is responsible for that information?"

3.0 Recommendations

Based on the findings of this report, world governments ultimately need to look at policies governing online practises and bring them into line with how the internet is used today. SNS's are taking advantage of dated governing laws to allow them to dictate user privacy policies, therefore exploiting users private and personal information without consent. "The globally recognized and accepted privacy fair practices essential for an effective online privacy policy are; Notice, Choice, Access, Security, and Enforcement" (McGrath, 2011). (See appendix 1 for an explanation of privacy fair practices)

SNS users are entering into a contract with sites by merely using the services of that site. Users must be aware of the terms of this contract by taking the time to read the privacy statement. It is the decision of the user as to whether he/she will continue to use the SNS, however informed or not most users will continue to use SNS's as they have become a significant means of modern communication and self expression. In light of SNS's leading position in this relationship, users must be very vigilant in what they choose to post on to SNS's as well as being aware of their personal privacy settings. In most cases SNS's have the legal right to use users personal information. If information posted to a site may at some time pose a potential security risk or threat then that information quite simply should not be posted.

Although SNS's are legally within their rights to conduct the practises that they choose to conduct, they should consider a more ethical, consumer-centric approach to their business. Privacy statements should be made clearer and more consistent across different SNS's, outlining in detail how user information will be used and by whom. SNS's are in a position where they can negatively impact on users lives by violating their trust and not sufficiently protecting their privacy. SNS's must consider their social and business responsibilities regarding the issues of user trust and privacy. It may come to the point where users have had enough and simply do not continue to provide SNS's with the personal information that they crave and deem to be so valuable.

References

Bateman, P. J., Butler, B. S., & Pike, J. C. (2010). To disclose or not: publicness in social networking sites. *Information Technology & People , Vol 24* (1).

Butler, E., McCann , E., & Thomas , J. (N.D). Privacy Setting Awareness on Facebook and Its Effect on User-Posted Content. *Human Communication , Vol 14*.

Dinh, A. K. (2011). Privacy and Security of Social Media in Health Care . *Journal of Health Care Compliance* .

Emerald. (2011). Facing up to Facebook Voyeurs. *Strategic Direction , Vol 27*.

Facebook. (N.D). *Facebook News room*. Retrieved March 18, 2012 from http://newsroom.fb.com/content/default.aspx?NewsAreaId=22

Grabner-Krauter, S. (2009). Web 2.0 Social Networks: The Role of Trust . *Journal of Business Ethics* .

Hooper, T., & Evans, T. B. (2010). The Value Congruence of Social Networking Services - a New Zealand Assessment of Ethical Information Handling. *The Electronic Journal Information Systems Evaluation , Vol 13* (2).

Hugl, U. (2011). Reviewing person's value of privacy of online social networking . *Internet Research , Vol 21* (4).

McGrath, D. L. (2011). Social Networking Privacy: Important Or Not? *Interdisciplinary Journal Of Contemporary Research In Business , Vol 3* (3).

Oxford Dictionaries. (2012). *Privacy*. Retrieved March 22, 2012 from http://oxforddictionaries.com/definition/privacy

Privacy. (2012, March 15). Retrieved March 21, 2012 from Wikipedia: http://en.wikipedia.org/wiki/Privacy#Privacy_law

Sangani, K. (2010). Who owns your personal data?

Tan, X., Qin, L., Kim , Y., & Hsu, J. (2011, April 19). Impact of Privacy Concern in Social Networking Websites.

US Legal INC. (N.D). *Privacy*. Retrieved March 21, 2012 from http://internetlaw.uslegal.com/privacy/

Appendices

Appendix 1 – Privacy Fair Practice Essentials (McGrath, 2011)

Each one of these elements provides a dimension of privacy protection for the user. Specifically, the five areas were defined for the subjects as given below.

Notice informs the user of what information is gathered about him/her, how it is used, and whether the site shares that information with others.

Choice declares whether the user is allowed options in the amount of information gathered and how that information may be used.

Access deals with providing the user a means to review collected data and correct it if needed.

Security refers to how information is safeguarded, along with other issues relating to integrity of information and to the site's computer related practices.

Enforcement relates to consequences imposed on a website for breech of the above fair practice elements of Notice, Choice, Access, and/or Security.