Original Article

Opinions of social web users on privacy and online DAM

Edgar Napoleon Asiimwe

is an Information Technologist. He holds a MSc Degree (Informatics) from Örebro University and Bachelors degree in Information Technology from Makerere University. He is the Co-founder and Director Finance & Human Resource, Projekt One Consult (U) Ltd and formally the Web Administrator/Part-time Lecturer at Faculty of Computing & IT Makerere University and Junior ICT Expert at MVP/UNDP, Uganda. His research interests are in E-Government (M-government), HCI & Usability, AT4E & ICT4D infrastructure.

ABSTRACT The web today hosts thousands of web user profiles. These profiles contain information, which is sensitive – a reason why the information is protected from illegal use by privacy policies. This kind of information is at times referred to as online digital assets. Online digital assets are either hosted on private or government websites and online systems depending on where users are registered. There is a possibility that after death or impairment of a user, the confidentiality of online digital assets may be compromised due to absence of ownership and weak legal policies. This may result into privacy infringement of the owner, that is, the deceased or the impaired as well as other people related to the affected user such as those that have had sensitive conversations with him or her. Using Facebook as a case study, this research examined social web users' opinions on privacy and online digital assets management (DAM) after death or impairment of a user. The study used an online questionnaire to collect opinions from 22 Facebook users. Results show that the majority of respondents consider privacy and online DAM to be important issues. On the other hand, other Facebook users think that privacy in social networking websites is a mere illusion. There are also users who are not familiar with the concept of DAM and do not have any means of managing their assets in case of impairment or death.

Journal of Digital Asset Management (2010) **6**, 312–318. doi:10.1057/dam.2010.37

Keywords: digital assets management; privacy; digital inheritance; social web; Facebook

INTRODUCTION

Digital content sharing, for example, text, video, photos and so on is one of the most drastic emerging online activities and has become a common practice in online communities.

Today, there is too much information owned by individuals in social networking websites some of which is sensitive. The fact that 'there is no absolute security',¹ information is subject to abuse by malicious users. People have begun to realize the need to protect and manage digital data using digital rights management (DRM)² and digital assets management (DAM) systems. DRM and DAM focus on protecting digital assets from all forms of mismanagement and are

possible solutions for problems related to digital inheritance. The concept of DAM emerged in 1990s as a result of accumulating assets that were in print form (p. 10).³ Today many organizations have implemented DAM systems to solve information, data mining and data storage as well as privacy problems.

Privacy and DAM are interrelated and are crucial issues in online content sharing. The private nature of some of the shared information makes data privacy an indispensable security requirement yet complex due to technology evolution.⁴ According to Sun *et al.*,⁷ data privacy is always at risk and requires protection. Privacy can be defined as the act of preventing an

Correspondence:
Edgar Napoleon Asiimwe
Swedish Business School,
Örebro University,
Sweden
E-mail: asiimwe@gmail
.com.

individual or group and their sensitive data from being viewed by others. In Bygrave,⁵ sensitive data is regarded as any private information about an individual or group that if compromised in regard to confidentiality, integrity and availability can have adverse effects to the individuals or groups.

The increasing popularity of social networks, for example, Facebook has raised several privacy concerns,⁶ although it is claimed that tools for protecting data are provided. This research aimed at examining social web users' opinions on privacy and online DAM after death or impairment of a user. We wanted to get answers on 'How should online digital assets be handled after death or impairment of social web users to protect their privacy?' so that no one else claims identity which may result into privacy infringements.

The rest of this article presents the research method, the results, a discussion on findings and conclusions.

METHOD

This study used a quantitative method, that is, online questionnaire as its research method. The questionnaire (Appendix), which comprised of 10 questions mainly focusing on two main themes (privacy and online DAM) was distributed to 50 Facebook users of which 22 out of 50 responded. These Facebook users were selected randomly from friends' list in my Facebook account. It was assumed that Facebook users have many digital assets online, as Facebook has been ranked the biggest sharing and social networking website in the whole world. Upon this reason, we chose it as our case study.

The online questionnaire was designed using Survey Monkey – a web-based tool for designing, collecting and analyzing data. However, data were analyzed using excel. This study was carried out in May 2010.

RESULTS

This section presents the results of the study. Demographics of respondents, view on privacy policies and online digital assets are some of the key aspects presented. In general, results indicate that Facebook users have many digital assets online such as videos, photos, applications and

so on, which they think require protection and proper management. However, a big percentage of respondents consider some of their online digital assets non-confidential thus they would not wish another person to manage them when they are unable to do so.

Demographics of respondents

The survey featured 22 respondents where 15 (68 per cent) males and 7(32 per cent) were females. All respondents were above 18 years of age. Out of 22 respondents 3 (14 per cent), 15 (68 per cent), 2 (9 per cent) and 2 (9 per cent) belonged to 18–24, 25–34, 35–49, and 50 and above age groups, respectively. The survey was circulated using Facebook e-mail facility by picking contacts from the user's list randomly. Therefore, feedback was received from Facebook users from different countries. Demographics of respondents are shown in Figures 1 and 2. While Figure 1 shows gender distribution, Figure 2 shows age groups.

Opinions on privacy policies

Privacy policies help users to understand the legal technicalities related to usability. Thus, they contribute to security awareness and protection of online digital assets. Respondent were required to state if they read Facebook privacy policies and why they do so. On the other hand, respondents who do not read privacy policies would state why they do not. As shown in Figure 3, 55 per cent of all

Figure 1: Respondents gender distribution (n=22).

Figure 2: Respondents age groups ($n=22$).

Figure 3: Users who read Facebook privacy policies ($n=22$).

respondents read privacy policies whereas the remaining 45 per cent do not.

Security reasons, privacy policy update notifications and curiosity to know the information contained in privacy policies are some of the factors that prompt users to read privacy policies. Figure 4 shows responses according to each factor.

Respondents who stated they do not read privacy policies (45 per cent) revealed that they do not do so for some reasons such as: (1) lack of time and interest, (2) laziness, (3) lack of alternatives to Facebook even if rules and policies were unfair, (4) cautiousness in usage, and most importantly (5) the perception that the privacy in social networking websites is an illusion.

Perceptions on online DAM

Facebook users have many digital assets on line. All respondents mentioned at least more than one example of information assets they possess on Facebook. These assets included photos (37 per cent), private messages exchanged with friends (35 per cent), applications (13 per cent), videos (11 per cent) and others (4 per cent). Within the category of other, fan pages and

calendar were listed. However these two can be categorised as applications. Figure 5 shows the most popular/owned Facebook digital assets.

Respondents were also asked to state how confidentially they perceive their Facebook assets to be. Sixteen per cent believe their information is very confidential, 28 per cent think their information is confidential, 24 per cent think it is less confidential while the remaining percentage (32) said their information is not confidential. Figure 6 shows Facebook users' perceptions on confidentiality of digital.

Some respondents justified their opinions by stating that they control who views what, using Facebook privacy tools and noted that some information is for universal sharing thus there is no agenda to hide information.

Facebook users were also asked if they think online DAM is an important issue that should be addressed in online communities. The biggest percentage (more than half) of respondents agreed, 4 per cent disagreed and 5 per cent do not know if the issue is important or not. Figure 7 shows the number of respondents according to their responses regarding the importance of online DAM.

A majority of respondents (43 per cent) cited that illegal access to their online information would compromise their privacy and the privacy of the people they communicate with and 25 per cent wished their online digital assets to remain secure when they are unable to manage them, for example, in case of impairment or death. Although the majority considered online DAM to be an important issue, 25 per cent of

Figure 4: Reasons that prompt users to read privacy policies ($n=22$).

Figure 5: Most owned digital assets on Facebook ($n=22$).

Figure 6: Perception on confidentiality of digital assets ($n=22$).

all respondents wished their assets should not be managed by someone else even when they cannot do it themselves. Figure 8 shows respondents' opinions regarding DAM after death, security and privacy.

On the question of what plans users have in case they are unable to access or manage their digital assets, many admitted that they do not have any plans and some had assumed that if they take long to use their Facebook accounts, their accounts would be deleted. On the other hand some respondents mentioned that they had not even thought about this issue.

To prepare for unforeseen circumstances that can prevent users from managing their online digital assets respondents suggested numerous strategies that included: having 'a next of keen' to claim rights after death, improving methods for content control and provide options for scheduled de-activation of accounts, forbidding users younger than 18 years from using Facebook, avoid publishing confidential information, sharing/giving access information to a trusted person, hiring digital assets managers or companies in DAM business, avoid using applications that require personal data and implement DAM legislations to protect the online community.

DISCUSSION

The findings show that social web networkers have strong concerns for privacy. Data privacy is an indispensable security requirement in online social networks,⁷ and most users utilize the available tools to protect their information from illegal use. Although there are many security measures for enforcing privacy, users still have little trust about security in social networking websites as revealed by the survey. In this regard, great understanding and new knowledge on information sharing is required,⁸ as users cannot predict all usage situations.⁹ One respondent is quoted to have said that: 'the concept of privacy on social networking websites is a mere illusion'.

Despite strong privacy concerns, some users do not read privacy policies. This is owing to constant changes in policies and too much influence of social network websites on the lives of people among other reasons. A user who seemed to have stopped reading policies noted that: 'I did it (read privacy policies) but they

Figure 7: Views on the importance of online digital assets management ($n=22$).

Figure 8: respondents' opinions regarding digital assets management after death, security and privacy.

change policies'. Another user who seemed to be fixated with social networks remarked that: 'I'll still need Facebook even if the rules are unfair'. This implies that the priority is to have Facebook but not privacy. All in all perceived loss of control may be a function of objective reality,¹⁰ for example, individual's subjective opinions and observations.

On the other hand, users are not familiar with DAM and most of them had not thought of digital inheritance of their assets as one user stated: 'I think this survey has drawn my attention to a lot of things, so I will begin planning the type of information I put on the web'. Although some users think online DAM is important and would entrust and insure digital assets and rights with another person, others expressed doubts and objections.

DAM literature shows that there is less research done on how to manage information

of individuals especially after death. As privacy continues to be a big challenge amidst growing social networks, DAM will become a critical aspect. Some websites, Facebook inclusive have implemented measures to protect people's information after death. For example, Facebook provides a form (accessed via Help Center >>Friends>>Suggestions) for users to report deceased friends. Another website (<http://www.entrusted.com>) manages individual digital assets after death. The approach of DAM to some extent protects people's privacy even when they are dead.

CONCLUSION AND RECOMMENDATIONS

In this article, we present and analyze Facebook users' opinions on privacy and online DAM after death of a user. In reflection of the research question, users are concerned about

privacy and recommend that, for online digital assets to be protected after death or impairment of social web users, the following should be done: (1) implement legislations for enforcing DAM after death, (2) improve methods for content control and provide options for scheduled de-activation of online accounts, (3) avoid publishing confidential information, (4) giving access rights to a trusted person, (5) avoid using applications that require personal data and so on.

In addition to the above users should try to use the available privacy tools on social websites. Use of privometer; a tool for measuring the amount of sensitive information leakage in a user profile is suggested in.⁶ This can help users on how to fix security loopholes. It is also intelligent to register with a DAM company if the user has not entrusted his/her assets with another trusted person.

REFERENCES

- 1 Merkow, M. and Breithaupt, J. (2005) *Information Security: Principles and Practices*, ISBN: 0-13-154729-1. Upper Saddle River, NJ: Prentice Hall Inc.
- 2 Petkovi, M. and Li, H. (2007) *Digital Inheritance of Personal and Commercial Content Using DRM*, 4th IEEE Consumer Communications and Networking Conference. Las Vegas; Piscataway, NJ: IEEE Press, pp. 950–954.
- 3 Austerberry, D. (2004) *Digital Asset Management: How to Realise the Value of Video and Image Libraries*, ISBN: 0240519248. Linacre House, Jordan Hill, Oxford: Elsevier Focal Press.
- 4 Kenny, S. and Korba, L. (2002) Applying digital rights management systems to privacy rights management. *Computers & Security* 21(7): 648–664.
- 5 Bygrave, L.A. (2002) *Data Protection Law: Approaching its Rationale, Logic and Limits*. The Hague, the Netherlands. Kluwer Law International.
- 6 Talukder, N., Ouzzani, M., Elmagarmid, K.A., Elmeleegy, H. and Yakout, M. (2010) *Privometer: Privacy Protection in Social Networks*, IEEE 26th International Conference on Data Engineering Workshops. Long Beach, CA; Piscataway, NJ: IEEE Press, pp. 266–269.
- 7 Sun, J., Zhu, X. and Fang, Y. (2010) *A Privacy-preserving Scheme for Online Social Networks with Efficient Revocation*, IEEE INFOCOM Proceedings. San Diego, California; Piscataway, NJ: IEEE Press, pp. 1–9.
- 8 Pardo, A.T., Gil-García, R.J. and Burke, B.G. et al (eds.) (2009) *Information sharing and public health: A case-based look at the ICT expectations – Reality gap. ICTs, Citizens and Governance: After the Hype!* 14: 180–197. <http://www.ctg.albany.edu/publications/bookchapter/infossharing/infossharing.pdf>.
- 9 Morin, J. and Pawlak, M. (2007) *A Model for Credential Based Exception Management in Digital Rights Management Systems*, Second International Conference on Internet Monitoring and Protection. San Jose, CA: IEEE Press, p. 41.
- 10 Hoadley, M.C., Xu, H., Lee, J.J. and Rosson, B.M. (2010) Privacy as information access and illusory control: The case of the face book news feed privacy outcry. *Electronic Commerce Research and Applications* 9(1): 50–60.

APPENDIX

Questionnaire – Social web users' opinions on privacy and online DAM after death or impairment of a user

The web hosts our sensitive information (online digital assets). The question is: If we lose control of our online digital assets, for example, we become impaired or die, do not we need someone to take care of our valuable information so that no one can claim it and use it for whatever they want? Using an example of Facebook, I would like to know your opinion on how online digital assets should be managed in case users are unable to access or manage them.

1. Which gender describes you?
(a) Male [1] (b) Female [0]
2. Age group
(a) Under 18 [0]
(b) 18–24 [1]
(c) 25–34 [2]
(d) 35–49 [3]
(e) 50 + + [4]
And how long have you been using Facebook? [state in months or years]
3. Do you read Facebook privacy policies?
(a) Yes [1]
(b) No [0]
4. If yes (4a), what prompts you to read privacy policies?
(a) Curiosity [0]
(b) Privacy policy updates notifications [1]
(c) Security reasons [2]
(d) Other (please specify) [3]
5. If no (4b), why?

6. Which of the following digital assets do you have in your Facebook account? [*tick whenever applicable*]
- (a) Photos [0]
 - (b) Videos [1]
 - (c) Private messages [2]
 - (d) Application [3]
 - (e) Others (specify) [4]

7. How confidential are these digital assets to you?
- (a) Very confidential [0]
 - (b) Confidential [1]
 - (c) Less confidential [2]
 - (d) Not confidential [3]

Please comment on your answer

8. The issue of online digital assets management is important
- (a) Strongly agree [0]
 - (b) Agree [1]
 - (c) Disagree [2]
 - (d) Strongly disagree [3]
 - (e) I don't know whether it's important or not [4]

9. I agree with the following statements [*tick only if you agree*]
- (a) I would need someone to manage my online digital assets in case I'm unable to do so [0]
 - (b) I wouldn't need someone to manage my online digital assets in case I'm unable to do so [1]
 - (c) I would want my online digital assets to remain secure even when I'm impaired or dead [2]
 - (d) Illegal access to my information would compromise my privacy and the privacy of those I communicate with [3]

10. What plans do you have for your Facebook information (digital assets) in case you are unable to access or manage it, that is, if you become impaired or die? and

What do you think users need to do in preparation for unforeseen circumstances that can prevent them from managing their online digital assets?