# Understanding Information Disclosure Behaviour in Australian Facebook Users

William Newk-Fon Hey Tow
Peter Dell
John R. Venable
School of Information Systems
Curtin University of Technology
Perth, Western Australia
Email: williamheytow@gmail.com, p.dell@curtin.edu.au, j.venable@curtin.edu.au

## Abstract

*The advent of social networking websites presents further opportunities for criminals to obtain information for use in identity theft, cyber-stalking, and worse activities. This paper presents exploratory research investigating why users of social networking websites willingly disclose personal information and what sorts of information they provide (or not). The study employed an ethnographic approach of participation in the online community and interviews of community members, combined with a quantitative survey. The findings show that users are often simply not aware of the issues or feel that the risk to them personally is very low. The paper recommends that government agencies or social networking websites themselves conduct campaigns to inform the public of these issues and that social networking websites consider removing some facilities. The study was conducted in an Australian context and focussed on the popular Facebook website.*

**Keywords**

Social networking websites, Facebook, privacy, information disclosure, identity theft

## INTRODUCTION

In 2007, after stealing the bag of a trainee teacher, a fraudster viewed the online profile of the victim and within three hours succeeded in obtaining more than £400 from her credit account (Gray and Montague 2007). Such cases are not isolated incidents; in 2006, a 20 year old woman received the following instant message: "Hey… I really like your Facebook pictures. You are very pretty. I look at your pictures every day and thought maybe we could meet sometime". Although she immediately blocked the sender, she received hundreds of e-mails regarding her interests, classes, and friends. Further, her mobile phone rang constantly and when she answered, all she heard was a clicking sound from a restricted number. The woman blamed the amount of uncensored self-information she had on her Facebook profile (Klein 2006).

Many jurisdictions have introduced laws to combat online abuse and required the owners of social networking sites to add more safeguards and privacy controls to protect users, including those in Australia. Bruce van der Graaf of the NSW Police Fraud Squad contends that merely knowing the identity and date of birth of the victim gives an identity thief the "key to the finance sector" (Stolen ID 2008). In 2003, the Attorney General of Victoria declared he would introduce the first cyber stalking law in Australia (Office of the Attorney General 2003). More recently, the Australian Federal Minister for Home Affairs also recommended that "making, supplying, using or possessing identity information, with the intention of committing an indictable offence, all become potentially indictable offences themselves" (Minister for Home Affairs 2008).

Indeed, both government and non-government organisations have campaigned to warn people not to disclose personal information online. Yet in an experiment conducted in August 2007 to explore how inclined Facebook users were to share information, 78% of 200 random friend requests sent on Facebook exposed their current address or location, and 41% of respondents were "happy to reveal all" (Sophos 2007), potentially exposing themselves to a range of threats including fraud, online and physical stalking and blackmail. In turn, this also exposes others to the risk of exploitation by identity thieves who, by using an identity for which they are not responsible, are unlikely to be held accountable for their actions.

Previous literature showed that social awareness and internet literacy influenced privacy concerns of Internet users (Dinev and Hart 2006). Though Hargittai (2008, p. 293) later confirmed that "online actions and interactions cannot be seen as tabula rasa activities, independent of existing offline identities. Rather, constraints on one's everyday life are reflected in online behaviour", a lack of knowledge still persisted in understanding why people deprive themselves of their privacy despite being warned about doing so. This research seeks to explain the information disclosure behaviour of users of the major social networking site Facebook, from their

perspectives and within their contexts. Such explanation could inform operators of social network systems such as Facebook and contribute to the development of policies and procedures to more effectively educate users.

The rest of this paper is organised as follows: The next section reviews previous research in this area. The third section then describes the research questions explored in this study. Next we describe the research method and the two subsequent sections discuss initial findings and detailed analysis respectively. The next section draws conclusions and makes recommendations while the final section acknowledges limitations.

## LITERATURE REVIEW

The phenomenon of publishing personal information online is relatively recent. When SixDegrees.com was launched in 1997, the website initially attracted millions of users but the website closed down in 2000 due to financial difficulties. Andrew Weinreich, founder of SixDegrees.com, stated that "SixDegrees was simply ahead of time" (Boyd and Ellison 2007). Current social networking sites however are enjoying massive success, which is likely to continue, at least in the medium term. Facebook is the most popular social networking site, and according to recent statistics the site has more than 100 million users (Facebook 2008). Such sites are receiving huge investments too; Facebook for instance, received a $240 million investment from Microsoft in 2007 (Malik 2007).In contrast to the increasing popularity of social networking sites, the degree of public concern about publishing personal information online appears to be falling: 56% of respondents to a study by Paine et al. (2007) were concerned about their privacy online, down from 70% of respondents who were asked similar questions by Jupiter Research in 2002. Campbell et al. (2001) also found that even though Internet users may express concerns about privacy, they still engaged in risky behaviours. In a survey carried out by the Computer Associates Inc. and the National Cyber Security Alliance (NCSA) of the United States, results indicated that of the 57% of participants of social networking websites who were aware of the risks of cybercrime, 74% had given out personal information such as e-mail address, name and birthday (Network Security 2006).

Another survey of North American college students revealed that although respondents ranked privacy policy higher than terrorism, almost 40% of the students who claimed to be concerned about protecting their class schedule still posted it on Facebook. The study concluded that there was "little or no relation between participants' reported privacy attitudes and their likelihood of providing certain information" (Acquisti and Gross 2006).

A vivid example of decreased concern for privacy is the increase in members' use of their real name as an online identifier, rather than the once-common use of pseudonyms or aliases. According to Gross et al. (2005), approximately 89% of the names on Facebook are valid, and it is this trend that has led some to describe Facebook as the "Google of people" (Jarvis 2007). Nevertheless, it is not only disclosure of real names that is the problem, since all kinds of data are published despite users' awareness of privacy issues.

Likewise, Govani and Pashley (2005) found that 84% of the participants were aware that they could change their privacy settings but less than 48% have made use of the privacy settings. Govani and Pashley (2005) further stated that even after making users more aware of privacy settings within Facebook, very few subsequently changed such settings to restrict who could access their information. Similar results were obtained by Strater and Richter (2007) with 67% of participants who had their profiles public not restricting access to their personal information to "only friends" and recently from Kolek and Saunders (2008) who found only 11% of Facebook users in their study restricted access to their profiles.

Govani and Pashley (2005) pointed out that in order to know why the Facebook users are disclosing personal information, it is important to examine the reason behind the use of the website, an action supported by Ellison et al (2007) who concluded that Facebook is used to maintain or intensify already existing relationships. According to Boyd (2006), the number of users of social networking sites continues to increase as teenagers respond to continually decreasing "access to public spaces" where they can be themselves, and among friends, thus prompting a desire to access virtual communities to "(re)create private and public youth space while physically in controlled spaces."

Undoubtedly, boundaries of public, physical spaces are clear; boundaries of virtual spaces are not. Drawing on Goffman (1959, 1963), Dell and Marinova (2002) argued that this would lead to more conservative disclosure of personal information online, due to difficulties delineating one audience from another. However, this theoretical prediction is at odds with the empirical evidence in which many users are willing to publish large amounts of personal information online for potentially the whole world to see.

This disconnect between user attitudes and behaviour is addressed by Lipford et al. (2008), who propose an improved tab interface in order to help users appreciate how various pieces of information are presented to different audiences. This allows users to more accurately understand which information is presented to whom, but

does not address the underlying issue when users deliberately choose to publish key pieces of information to a wide audience.

Such decisions are essentially the result of decreasing concern with online privacy issues, which, as discussed above, has led to a situation in which millions of users are at risk. The Information Commissioner's Office in the United Kingdom states that 4.5 million people aged 14 to 21 are putting them at risk of identity fraud or ruining their future careers by posting private information in social networking sites (Brooks 2007).

Banning the use of social networking websites is practically impossible and undesirable, so programmes to promote awareness of the dangers of disclosing personal information are imperative. Initiatives like the NetAlert – Protecting Australian Families Online or Get Safe Online in the United Kingdom are a significant step in the right direction, although given the willingness of users to publish personal details online, their effectiveness to date may be limited.

Understanding how such programmes can be improved requires understanding of what motivates people to engage in risky online behaviours. Although previous research has identified the scale upon which such behaviours occur, there is little understanding of why people knowingly choose to disclose information that may expose them to risk. This research gap forms the basis for the current project, for which specific research questions are described in the next section. The project also contributes to improved theoretical understandings, by resolving the contradiction between the theoretical prediction noted above and the empirical evidence.

## RESEARCH QUESTIONS

With a view to determining how Facebook users value their privacy, this project investigates why users choose to disclose personal information despite warnings about doing so, and evaluates users' awareness of the risks to which they are exposed. There is a need to know whether the users are consciously making themselves exploitable and the reasons for it, or the users are yet to be alerted, thus verifying that the campaigns have been putting across the message of caution effectively. Accordingly, the following research questions are asked:

Online Privacy:

- What personal information do Facebook users have on their profiles?
- What value do Facebook users place on their online privacy?
- Why do Facebook users publish personal information online?
- How and why do Facebook users limit or restrict access to their personal information?

Awareness:

- Are Facebook users aware of the risks of publishing personal information?
- Do Facebook users feel safe online?

## RESEARCH METHOD

Past research has identified a problem vis-à-vis users of social networking sites publishing personal information online and thus exposing themselves to potentially serious risks. The purpose of this study is exploratory rather than descriptive, and seeks to obtain a clearer understanding of why users would do this, culminating in the creation of an explanatory model. The model proposed represents the phenomenon and has no predictive power. In order to learn what is relevant to the population, the interpretive paradigm was adopted.

The research progressed through three stages conducted from March to May 2008. The objective of the first stage was to go where the users are and appreciate the state of being a member of Facebook. One of the authors immersed himself in the Facebook community; essentially, this involved taking on the role of an "introspective observer" (Denzin 1971) in order to better understand the Facebook community from the point of view of a participant. Thus, a Facebook account was created and linked to the Australia 'Network', which at the time the research was conducted was the only way for people to search users based on gender, age groups, religious and political views, interests and other factors. (Facebook has recently removed all 'Network' pages and promoted the use of 'Groups' instead, which currently have no browse feature.) The researcher also modified his profile, adding his name, date of birth, photos, education history so as to fit seamlessly in the context of the population.

The observations obtained during the first research phase were explored in a more generalisable way in the second, survey phase of the research in which a questionnaire was developed and sent to users of the website. The purpose of the questionnaire was two-fold; obtain the views of more Facebook users to grasp a broader view of the situation and refine the focus for the later stage of the research. Since it was not possible to obtain a mailing

list of all Facebook users for random sampling, the snowball sampling method was used during this phase. As Salganik and Heckathorn (2004: 196) explain, "the basic idea behind these methods is that respondents are selected not from a sampling frame but from the friendship network of existing members of the sample." Data from the survey were analysed using quantitative data analysis methods, including measures of central tendency and associations between variables.

Results from the questionnaire identified key issues for the researcher to address in the case studies that followed in the third and final stage. Online interviewing was chosen as the most suitable method to investigate the research questions, not only because no other method would have a similar ability to build a relationship between the respondent and the researcher but also because interviews enabled the researcher to consider "local conditions and local values" (Lincoln and Guba 1985: 40). Participants were contacted both through the mailing system of Facebook and through word-of-mouth.

In the third stage, in-depth, ethnographic interviews were conducted with Facebook users to investigate issues surrounding privacy, disclosure of information online, and awareness of the risks. The sample of interviewees was not intended to be representative in a statistical sense. Rather, the objective was to reach users of different gender, age groups, relationship status and profile accessibility. The sample also included past victims of stalking and identity theft. The aim was to cover the diversity of users rather than to generalise. Purposive sampling was chosen because this method enabled the researcher to encompass as large a scope of data as possible. Sampling was stopped when informational redundancy (saturation) had been reached.

The ethnographic interviews followed two phases: building rapport with participants, followed by eliciting information. Strong rapport is beneficial to interview researchers as it fosters a basic sense of trust between interviewer and interviewee and permits a freer flow of information (Spradley 1979). To build rapport the researcher began with general, conversational style questions such as "How long have you been using Facebook?", as well as Grand Tour Questions (Spradley 1979). This was subsequently followed by more specific, research focused questions aimed at eliciting data directly related to the research questions.

The qualitative interview data were analysed using domain analysis (Atkison and Abu El Haj 1996). Domain analysis focuses entirely on qualitative data and "allows the participants to identify for themselves the topics and issues of importance" (Atkison and Abu El Haj 1996, p. 438), and aims "to reconstruct the categories used by subjects to conceptualise their own experiences and world view" (Goetz and LeCompte, cited in Lincoln and Guba 1985: 335). The domain analysis involved four steps, which yielded a model that was grounded in the data, rather than imposed from a theoretical perspective.

First, the responses of the interviewee were segmented into 'units of meaning', where a unit is the purpose or the subject of the interviewee's comments. The second step organised the units of meaning into preliminary categories, making sure to include sufficient information about the context from which the units of meaning were derived (Seaman 1999). In the third step, the preliminary categories were refined and consolidated to obtain a list of the dominant categories, or domains. Once the domains had been identified, the researcher could then rearrange the units of meaning into their respective domains. Finally, the researcher was able to investigate if there is evidence of relationships between the domains – particularly evident in cases where units of meaning appear to belong in more than one domain. This process, in which qualitative data were analysed and re-analysed, was laborious and time-consuming. However, this was particularly valuable as it helped the researcher to obtain a clearer understanding of the data and also to correct any mistakes made during the earlier steps.

The output of this domain analysis was a model of the key concepts affecting users' information disclosure behaviour, and the relationships between those concepts.

The next section describes the data gathered during the three research stages and initial findings.

## INITIAL RESULTS

300 profiles of users under the Australia 'network' were viewed using Facebook's browse feature. Over 50 hours were spent observing daily life on Facebook. Not only could the researcher view profiles of many other people, but he was able to do so without the knowledge of the individuals whose profiles were being viewed. Personal information that could be read straight from profiles included name, relationship status, friends list, photos, date of birth, work and education history. The comment feature of Facebook, the 'Wall', was also a rich source of information about the current activities of users, although the messages were typically quite brief.

Facebook explicitly asks its members to describe the relationship they have with each other, such as 'In my family', 'We dated', 'Worked together' and so on. This relationship information can prove to be valuable for social engineering criminals. For example, assuming person A leaves his profile public, criminal Z may be able to view who A travelled with, who A lived with, who A went to school with and even identify A's partner, family

and colleagues. Armed with such information, criminal Z will able to fabricate a profile to misrepresent A or to obtain further information on A by acting on A's behalf.

The questionnaire used in the second stage consisted of a mix of multiple choice, dichotomous and open-ended questions pertaining to, the methods used to secure personal information, the reasons for use of social networking websites, the information users are willing to share and users' understanding of cybercrime 'phishing'. From the 215 individuals who received the questionnaire, 51 responded, giving an overall response rate of 23.7%. When asked about their use of social networking websites like Facebook, 45 respondents out of the 51 (88%) said they used the websites to "keep up with my friends and family". While 34 respondents (67%) claimed restricting access to their profiles, 16 (31%) selected "I don't put any personal information", seven (14%) reported not protecting their personal information and only one (2%) admitted putting fake information on her or his profile.

Among the 35 respondents (69%) who attempted to explain the term "phishing", only six (12%) could accurately describe the term. The top three pieces of information users were least willing to disclose online were physical address (43 out of 51 or 84%), full name (40 out of 51 or 78%), and contact number (39 out of 51 or 76%).

Table 1. Information users are willing to post online

| | Yes | No |
|---|---|---|
| Full Name | 11 | 40 |
| Date of Birth | 37 | 14 |
| E-mail | 36 | 15 |
| Home Address | 8 | 43 |
| Personal Contact Number | 12 | 39 |
| Work Information | 18 | 33 |

In the third stage, interviews with 25 individuals were undertaken; 18 of which were contacted and interviewed through Facebook's mailing system and the remaining seven of which were contacted through word-of-mouth and interviewed face to face and through phone calls. The sample consisted of people of different relationship status, aged from 21 to 50, included users who had fake information on their profiles and who were victim of stalking and impersonation. Data collected also came from users who claimed not to use social networking websites and users with more than 300 connections.

More detailed analysis is described in the following section.

## DETAILED ANALYSIS AND RESULTS

Users reported publishing an average of 2.25 types of information out of a total of six types of information examined in the questionnaire (name, date of birth, physical address details, e-mail, contact numbers and work information). Analysis using Pearson Chi-Squared testing found that there was a statistically significant relationship ($\alpha = 0.05$) between belief of the user being safe from identity theft and the number of information types the user was willing to publish online ($p = 0.047$). Table 2 below summarises these results.

Table 2. Fisher's Exact Test value

| | Value | df | Asymp. Sig. (2-sided) | Exact Sig. (2-sided) | Exact Sig. (1-sided) |
|---|---|---|---|---|---|
| Pearson Chi-Square | 5.853(b) | 1 | .016 | | |
| Continuity Correction (a) | 3.951 | 1 | .047 | | |
| Likelihood Ratio | 5.239 | 1 | .022 | | |
| Fisher's Exact Test | | | | .028 | .028 |
| Linear-by-Linear Association | 5.738 | 1 | .017 | | |
| N of Valid Cases | 51 | | | | |

a. Computed only for 2x2 table
b. 1 cell (25.0%) had an expected count less than 5. The minimum expected count is 2.20.

Similarly, there was a significant correlation between the belief of being safe from identity theft and publishing of physical address details of the user ($\chi 2 = 5.833$, $p = 0.016$). Due to low values in some cells of the cross-tabulation, this was verified using Fisher's Exact test ($p = 0.028$), which can be used if one or two of the cells in a 2x2 cross-tabulation have values lower than 5.

This finding demonstrates that the level of awareness of the risks had some influence on users' information disclosure behaviour – if users do not feel safe, they are less likely to disclose physical address information, and more likely to disclose fewer pieces of information in total. However, these relationships were weak, and there was no significant relationship between perceived safety and disclosure of any of the remaining five types of information.

The third research stage further explored what drives users to publish personal information online. The domain analysis process described above yielded three key concepts arranged in a model of users' information disclosure behaviour, shown in Figure 1 and explained below.

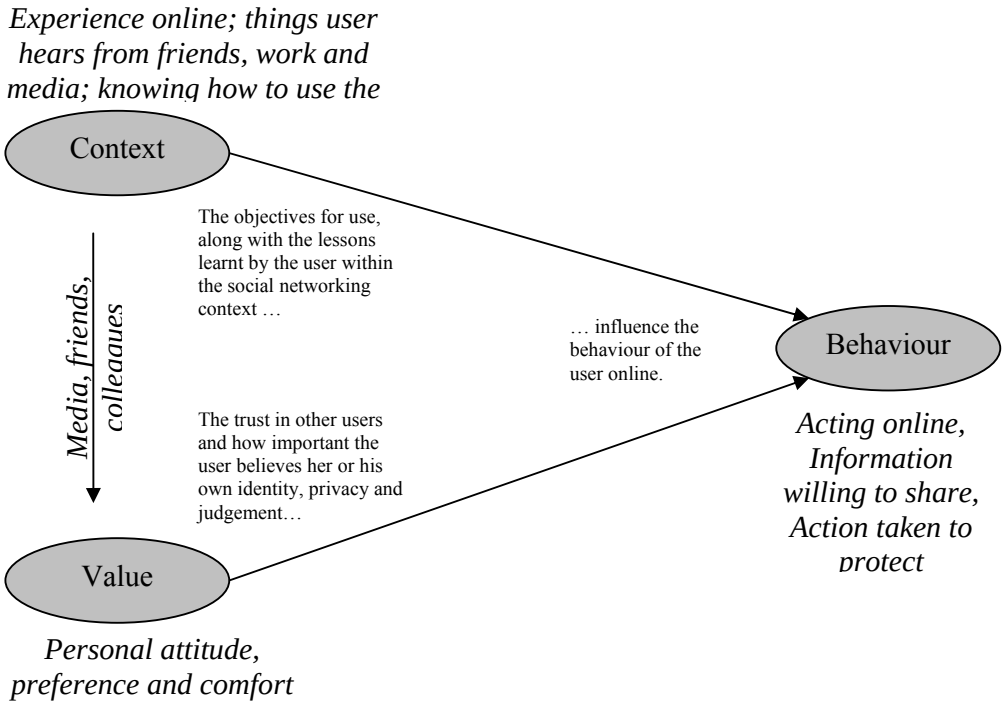


Figure 1: Model of users' information disclosure behaviour

The above model contains three domains that emerged from the data analysis: Context, Value and Behaviour. Context includes contextual factors that influence users' information disclosure behaviour. This includes a user's objectives for using social networking sites in the first place, as illustrated in the following quotations. (Note: Quotations from online interviews are reproduced verbatim, including spelling and grammar errors, which are common in chat and message facilities.)

> "i only use Facebook to keep in contact with my friends" (interview participant)
>
> "I use my Facebook as a kind of CV." (interview participant)

Context also includes outside influences, such as friends, co-workers, mass media, as well as previous personal experience, all of which can make an individual user aware of the risks of publishing personal information online.

> "i guess in a way i spose from tv, ads and people tlking you learn that its not such a safe thing to put everything up about yourself" (interview participant)
>
> "i think i am the same offline perhaps more vigilant online though because you hear so many horror stories." (interview participant)

The second domain, Value, refers to each individual user's values relevant to their personal sense of privacy. Value can be shaped by Context as individuals are influenced by the media and others around them. Value includes the value individuals place on their own privacy, as illustrated in the following comments.

> "I'm a fairly private person generally, and don't easily let new people into my inner circle" (interview participant)

> "I tend to keep things pretty priviate when it comes to online sites such as Facebook" (interview participant)

Value also encompasses the value users place on their own identity and whether they consider themselves a likely target for identity theft. The naïve belief that a normal, unremarkable person's identity has no value to an identity thief was common.

> "i don't think anyone would want my identity!" (interview participant)

> "guess I figure my identity isn't worth stealing - I'm probably a bit naive/blase about that." (interview participant)

Value also covers a user's sense of trust in the "generalised other" (c.f. Mead 1934), as exemplified in the following quotations.

> "I guess I trust that the people on Facebook will do the right thing and not abuse the concept" (interview participant)

> "It's the trust factor really you don't know who you can trust these days" (interview participant)

Context and Value both influence a user's Behaviour – the third domain to emerge from the domain analysis process. The relationship between Value and Behaviour is clear and intuitive – if a user is uneasy about others knowing their personal details in general, they are unlikely to post those details online.

> "I do worry about publishing my personal info" (interview participant)

However, the interviews revealed relatively few cases where users had this kind of concern. Most were willing to post information because their objective was to communicate with family and friends and were unaware of the risks involved, as in the following example.

> "Full name for searchability-so friends can find me" (interview participant)

However, if users had heard stories of identity theft, they would also be less likely to divulge their own details, as in the following example.

> "Identity theft would be one of my concerns and that is why I never publish more full details nor do I publish everything correctly their are purposeful mistakes." (interview participant)

This is a key finding as it provides an explanation for the contradiction between empirical evidence and the theoretical prediction of Dell and Marinova (2001): that users are only likely to become less likely to divulge personal information online when they become aware of and appreciate the risks of doing so. The boundaries to social situations are far less obvious than they are in face-to-face interaction; as Meyrowitz (1990) notes, online situations are essentially the patterns of access to information, and as such they may be convoluted or invisible.

Technical solutions, such as that proposed by Lipford et al. (2008) can help reveal these boundaries. The current research also indicates that users more fully comprehend the boundaries are a consequence of experience, perhaps by having one's information misappropriated or perhaps by hearing of such cases. A final, interesting example of how personal experience can affect a user's information disclosure behaviour was triggered by the research itself.

> "d.o.b i guess i 'thought' it was harmless... however now that i am thinking about it... i am going to delete it." (interview participant)

This demonstrates that it is possible to alter users' behaviour through education. It seems that the "default" behaviour of users is typically to publish information for the benefit of others, and it is only after information about identity theft and associated risks is communicated that users will consider altering their behaviour. This insight has led to the recommendations in the following section.

## CONCLUSIONS AND RECOMMENDATIONS

The findings in this paper correspond with those from previously mentioned research and enrich theoretical understandings of online information disclosure behaviour. As Dinev and Hart (2006) demonstrated, a relationship exists between social awareness and Internet privacy concerns. Undeniably, the suggestion from Thierer (2007) that "education is absolutely essential" still holds true. People should be reminded that they have control over what they put on their profiles.

Knowing what influences the users to post personal information online empowers governments and relevant authorities to tackle the root of the problem. This research adds two new recommendations to the body of advice for designers of social networks systems:

- First, many users have a naïve sense that online communities are safe. Therefore, social networking sites such as Facebook should more effectively communicate to users the risks involved with divulging personal information. Further, such sites should consider reviewing whether certain types of information – date of birth, for example – should be made public at all, and whether sites should be modified to prohibit doing so.
- Second, in the same way that other public information campaigns have used real-life cases, government and other organisations responsible for public information campaigns should consider communicating examples of identity theft and other, similar issues.

It is the authors' hope that by following these recommendations, the overall risk of identity-related crimes will be reduced.

## LIMITATIONS

All studies have their limitations, and this one is no exception. First, it should be noted that this study limited itself to the Facebook online community. To conduct in-depth, ethnographic analysis of multiple communities would be a very large project and was beyond the scope of the research reported in this paper. However, such work would be valuable in order to determine whether the findings in this study can be applied more broadly, and to reveal subtle differences (if any) between different communities.

Likewise, the study was restricted to Australian users and should be replicated in other national and cultural contexts, to determine if the findings can also be applied internationally.

Further, this study did not investigate individual attitudes toward risk, which will inevitably affect users' decisions to disclose information. Further investigation of the way different users' attitudes toward risk affect their online information disclosure behaviour is clearly warranted in future work.

## REFERENCES

Acquisti, A. & Gross, R. 2006. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook, Proceedings: 6th Workshop on Privacy Enhancing Technologies, Springer, Berlin, pp. 36-58.

Atkinson, S. & Abu El Haj, M. 1996. Domain analysis for qualitative public health data, Health Policy and Planning, Vol. 11, No. 4, pp 438-442.

Boyd, D. 2006. Identity production in a networked culture: Why youth heart MySpace, Conference paper talk at AAAS 2006 (part of panel: "It's 10PM: Do You Know Where Your Children Are … Online!"). St. Louis, Missouri: February 19, 2006.

Boyd, D.M. & Ellison, N.B. 2007. Social Network Sites: Definition, History, and Scholarship, Journal of Computer-Mediated Communication, Vol. 13, No. 1, Article 11.

Brooks, G. 2007. Secret society, New Media Age, 13 December, p. 10.

Campbell, J., Sherman, R.C., Kraan, E. & Birchmeier, Z. 2001. Internet Privacy Awareness and Concerns among College Students, Paper presented to APS, Toronto, June 2001. Available from http://www.users.muohio.edu/shermarc/ aps01.htm.

Dearne, K. 2007. ID thefts brings tech to the fore in law, Australian, 18 September, p. 21.

Dell, P. & Marinova, D. 2002. Erving Goffman and the Internet, Theory of Science, vol. 24, no. 4, pp. 85-98.

Denzin, N.K. 1971. The Logic of Naturalistic Inquiry, Social Forces, Vol. 50, No. 2, pp. 166-182.

Dinev, T. & Hart, P. 2006. Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact, International Journal of Electronic Commerce, Vol. 10, No. 2, pp 7-29.

Ellison, N.B., Steinfield, C., Lampe, C., The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites, Journal of Computer-Mediated Communication, vol. 12, iss. 4.

Facebook 2008. About Facebook, accessed 7 April 2008, from http://www.Facebook.com/about.php.

Goffman, E. 1959. The Presentation of Self in Everyday Life, Anchor Books, New York.

Goffman, E. 1963. Behavior in Public Places, The Free Press, New York.

Govani, T. & Pashley, H. 2005. Student Awareness of the Privacy Implications When Using Facebook, unpublished manuscript, Available from http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf.

Gray, R. & Montague, B. 2007. Criminals Trawl Facebook and MySpace, The Telegraph (UK), Available from http://www.telegraph.co.uk/news/uknews/1558125/Criminals-trawl-Facebook-and-MySpace.html.

Gross, R., Acquisti, A. & Heinz, H.J. III 2005. Information Revelation and Privacy in Online Social Networks (The Facebook case), Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, ACM, New York, pp. 71-80.

Hargittai, E. 2008. Whose Space? Differences Among Users and Non-Users of Social Network Sites, Journal of Computer-Mediated Communication, Vol. 13, Iss. 1, pp 276–297.

Jarvis, J. 2007. Amazing Facebook, Available from http://www.buzzmachine.com/2007/05/29/amazing-Facebook/.

Jones, H. & Soltren, J.H. 2005. Facebook: Threats to Privacy, MIT, Available from http://www.swiss.ai.mit.edu/6.805/student-papers/fall05-papers/facebook.pdf

Kahn, C.M. & Roberds, W. 2008. Credit and identity theft, Journal of Monetary Economics, Vol. 55, No. 2, pp. 251-264.

Klein, A. 2006. Facebook Opens Too Many Doors?, Planet Blacksburg, Available from: http://www.planetblacksburg.com/news/klein-Facebook-042606.html.

Kolek, E.A. & Saunders, D. 2008. Online Disclosure: An Empirical Examination of Undergraduate Facebook Profiles, NASPA Journal, vol. 45, no. 1, pp 1-25.

Lincoln, Y.S. & Guba, E.G. 1985. Naturalistic Inquiry, Sage Publications, California.

Lipford, H.R., Besmer, A. & Watson, J. 2008. Understanding Privacy Settings in Facebook with an Audience View, Proceedings: Usability, Psychology and Security '08, Available: https://www.usenix.org/events/upsec08/tech/full_papers/lipford/lipford.pdf.

Malik, O. 2007. Facebook launches Mobile, Takes $240 Million Investment from Microsoft, Available from http://gigaom.com/2007/10/24/Facebook-and-microsoft-bff-for-240-million/.

Mead, G.H. 1934. Mind, Self and Society: From the Standpoint of a Social Behaviorist, University of Chicago Press, Chicago, IL.

Meyrowitz, J. 1990. Redefining the situation: Extending dramaturgy into a theory of social change and media effects. In Riggins, S.H. (ed), Beyond Goffman: Studies on Communication, Institution and Social Interaction, Mouton de Gruyter, Berlin.

Minister for Home Affairs 2008. New Identity Crime Offences Proposed [media release], Available from http://www.ministerhomeaffairs.gov.au/www/ministers/ministerdebus.nsf/Page/MediaReleases_2008_Firstquarter_27March2008-Newidentitycrimeoffencesproposed.

Network Security 2006. 'Social networking' study shows cybercrime risk, Network Security, Vol. 2006, Iss. 11, November 2006, p. 2.

Office of the Attorney General 2003. Australia's First Cyberstalking laws [media release], Available from http://www.legislation.vic.gov.au/domino/Web_Notes/newmedia.nsf/bc348d5912436a9cca256cfc0082d800/2550a989153b5bebca256cf600824ef2!OpenDocument

Paine, C., Reips, U.D., Stieger, S., Joinson, A., & Buchanan, T. 2006. Internet users' perceptions of 'privacy concerns' and 'privacy actions', International Journal of Human-Computer Studies, Vol. 65, No. 6, pp. 526-536.

Salganik M.J. & Heckathorn D.D. 2004. Sampling and estimation in hidden populations using respondent-driven sampling, Sociological Methodology, Vol. 34, No. 1, pp. 193-240.

Seaman C.B. 1999. Qualitative Methods in Empirical Studies of Software Engineering, IEEE Transactions on Software Engineering, Vol. 25, No. 4, pp. 557-572.

Sophos 2007. Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves, [media release], Available from http://www.sophos.com/pressoffice/news/articles/2007/08/Facebook.html.

Spradley, J. 1979. The Ethnographic Interview, Holt, New York.

Stolen ID 2008. television program, SBS Television, Australia, broadcast 19 May.

Strater, K. & Richter, H. 2007. Examining Privacy and Disclosure in a Social Networking Community, Symposium On Usable Privacy and Security (SOUPS) 2007: Proceedings of the 3rd symposium on Usable privacy and security, July 18-20, 2007, Pittsburgh, USA.

Thierer, A. 2007. Social Networking and Age Verification: Many Hard Questions; No Easy Solutions, Progress & Freedom Foundation, No. 14.5.

## ACKNOWLEDGEMENTS

The authors would like to acknowledge the helpful comments and suggestions from the anonymous reviewers.

## COPYRIGHT