Control, Risk Awareness and Self-Disclosure: Factors Influencing Online Privacy

Arthur Joel Lewis[1]

University of Auckland,

Department of Computer Science,

Email: alew525@aucklanduni.ac.nz

23rd October, 2013

Abstract

Online privacy is an issue which cannot be ignored today owing to the widespread use of the Internet in today's Information age. Possible misuse and leakage of sensitive information pertaining to an individual or an organization may potentially result in catastrophic losses. This paper casts some light on the various factors that play an influence on deciding privacy requirements in a given online setting. It analyzes some work done in existing literature as well as links them together by comparing the problems put forth by them. Limitations of my analysis and some motivation for future work in this regard are also discussed.

[1] Arthur Joel Lewis is a Post Graduate Student at the University of Auckland, currently pursuing a post graduate diploma in Computer Science

1 Introduction

Online privacy is an issue which has and will always continue to be addressed by policy makers, industrial organizations and security analysts. However, this issue has opened up new vistas over the past decade due to the emergence and growth of social networking sites such as Facebook and Twitter [3], [4]. According to [2], people feel assured about security of their information if they are given some level of control over its release. As a result, policy makers are going over the top to make users in charge of their private information by introducing solutions which give users as much as control as possible over the release of sensitive information in an online setting.

However, a recent study by Brandimarte *et al.* [2] pointed out that mere control might not be sufficient to address privacy. This study introduces a psychological argument with respect to the issue of privacy concerns existing among people. It points out that increased levels of control would end up back firing since users would have a "perceived sense of control" over their personal information and this would prompt them to be more likely to divulge the same. This perceived sense of control would make them completely forget about the risks associated over the release of information, thus, resulting in a paradox coined as a "control-paradox" by the study's authors.

So, a question came into my mind in this regard i.e. do policy makers have to change their stance about granting users more control to uphold privacy? This paper discusses my views on this matter by analyzing some studies that would help answer my question.

2 The Perception of Control

The premise of my analysis is based on the work done by Brandimarte *et al*. However, the focus of my analysis is not just confined to the problem pointed out by [2] alone but also considers another problem which Spears *et al.* [5] attempts to address. The former indicates a potential problem owing to human psychology while the latter talks about another problem which can strongly be linked to the one pointed out by the former.

The research conducted by [2] presents a psychological point of view with respect to the issue of online privacy. It focuses primarily on the aspect of "perceived control" which users end up treating as actual control over personal information. As a result they end up developing a superficial attitude which makes them overlook other aspects such as the risks associated with the disclosure of information. These risks are linked to consequences that might arise if this information is accessed by other parties once it is divulged by the user. So Laura Brandimarte and her colleagues make a hypothesis which states that a greater sense of control over the disclosure of sensitive information distracts users from the bigger picture i.e. the associated consequences of careless disclosure resulting in them to be all the more likely to reveal more. This hypothesis is supported by the three surveys conducted in their study.

There are a few possible limitations of the first two surveys conducted in this work. These two surveys involved university students answering some personal questions to publish their profiles in a social networking website. These questions varied in levels of intrusiveness i.e. the degree to which information can be sensitive. A measure of intrusiveness was determined on the basis of a former study done on the same population. However, details of this analysis were not mentioned in the paper. The level of intrusiveness can also vary from one individual to another. So, this might have had some bearing on their final results. Moreover the students were from different ethnic groups and hence, some information that could ordinarily be deemed sensitive by one ethnic group need not be so by another [6]. Nevertheless, their hypothesis was apparently supported by the results of these studies since it backed the notion of decreased control resulting in reduced willingness to divulge information despite the risks associated with disclosure being drastically reduced.

Students were divided into two groups for the first survey. One group was told that their information was going to be surely published online (thus giving them a greater sense of control), while the other group were informed that only information pertaining to some random 50% of the total participants will be published (hence, a lesser sense of control). The results backed their hypothesis but this could be owing to students craving for some amount of publicity. So in my opinion the results produced by the first study were not conclusive as the study did not take into account factors such as online publicity to boost popularity among peers.

So the second survey extended the first by introducing the aspect of accessibility of their information. Students were subdivided into categories where they were told that their details would be accessed by either students alone or by both the students and the faculty. Once again each category of students was divided into the two control groups. Naturally, it was expected for students in the category where information was to be accessed by faculty to be a bit cautious about answering some questions which would be intrusive as they would prefer their faculty not knowing about it. However, since this category was subdivided into two groups, the group which perceived greater control ended up disclosing more information of a sensitive nature as compared to the group which perceived lesser control. Two possibilities can exist for this behavior. Firstly, the students in the group which perceived lesser control would have panicked about answering intrusive questions since they would have been in a state of uncertainty about the information being accessed despite the associated risks being curtailed by 50%. As I mentioned earlier, the other possibility is that students would have been craving for some campus wide publicity and hence, would have shown some disinterest in answering much of the questions which were labeled as “intrusive”. Taking into account that the mean age of these students was around 21.5 years old, the second possibility might have been all the more likely as there would have been some rowdy bunch of students craving for some popularity among their peers as well as some level of notoriety among the faculty members by publishing some infamous facts about themselves.

The third survey consisted of students from the same population anonymously answering yes/no questions pertaining to ethical behaviors i.e. whether they consumed drugs, smoked or things of that nature. They were given the option of not answering a question and were informed in adavcne about their answers being published on a research bulletin. Four levels of control were introduced in this survey with each level introducing a more fine grained sense of control than the previous one. One of these levels of control also prompted students to publish their demographic information along with their answers. This was risky as it could end up increasing the likelihood of establishing a student’s identity. Nevertheless, the more fine grained the level of control perceived by students, the more willingness they displayed to divulge information. But will this hold for all kinds of age groups? People’s concerns about personal privacy may also vary as per their age and income groups. This study did not take into account a more representative sample consisting of people belonging to different age groups. Also as I have mentioned before, the aspect of a question’s “intrusiveness” was a critical element in this study and the determination of the measure of intrusiveness was not explained. Hence, this would have had some bearing on the results. However, to the best of my knowledge this study adopted a novel approach to point out a new issue with respect to online privacy.

3 The Necessity of Risk Awareness

The work undertaken by Spears *et al* [5] talks about resolving online privacy issues by presenting another problem which is different from the one discussed in [2]. However, the problem discussed here can be effectively linked to the problem discussed by Brandimarte’s work as it implicitly extends the problem discussed by Brandimarte. It consider two factors i.e. notifying online consumers about what would happen to their personal information while performing online transactions and raising the awareness of the potential risks involved. This work clearly asserts that these two aspects are not synonyms of each other and the former among the two is not sufficient to guarantee online privacy.

This study states that mere notices which convey information about online privacy policies are not sufficient for consumers to be fully aware of the associated risks. The paper takes into account several factors associated with online consumer privacy such as the risks involved and by extension the threats that accompany them. A privacy risk is termed as the expectation of losses linked with the disclosure of personal information whereas a threat to privacy can be referred to a circumstance or activity which has the potential to bring about such losses [1]. Instances of losses associated with the disclosure of information include unauthorized parties accessing your personal information (stealing), misrepresentation of your information as well as its illicit or inappropriate usage. Risk management of online privacy threats by online consumers is the premise of this work.

Risk management is a two phase process which consists of risk assessment and risk treatment. The former involves identifying the potential threats and prioritizing them. Once this is done, the latter is concerned with performing necessary actions to treat the identified threats in an appropriate manner. The treatment process consists of either:

a) *Risk Mitigation: A proactive way to reduce risks by taking up counter measures while still continuing to perform a risky activity such as online shopping. For instance, installing special software to curb threats to privacy*
b) *Risk Avoidance: A preventive way to reduce risks by not performing a risky activity in the first place*
c) *Risk Acceptance: This is a passive approach unlike Risk Mitigation as it assumes nothing will go wrong and accordingly no measures are taken to lower risk. This is usually practiced if avoidance and mitigation incur costs that would outweigh the benefits associated with them.*

In order to enable consumers to manage privacy risks, the risks need to be first identified via a notice which informs the online consumer about who (the online entity) the data will be shared with and for what purpose. So this notice gives them a choice to opt in or out of the online transaction. This is analogous to giving users control over the release of their information as explained in [2]. However, a notice fails to explain potential losses that would incur if this information is used inappropriately. In other words a notice fails to explain the associated risks involved with disclosure of this information. This argument strongly relates to the problem conveyed by Brandimarte *et al* [2] i.e. the potential consequences (or threats) that might arise after this information is disclosed by the user. But a notice does give users an idea about the online entity's information privacy practices which pertain to the security of consumer's information.

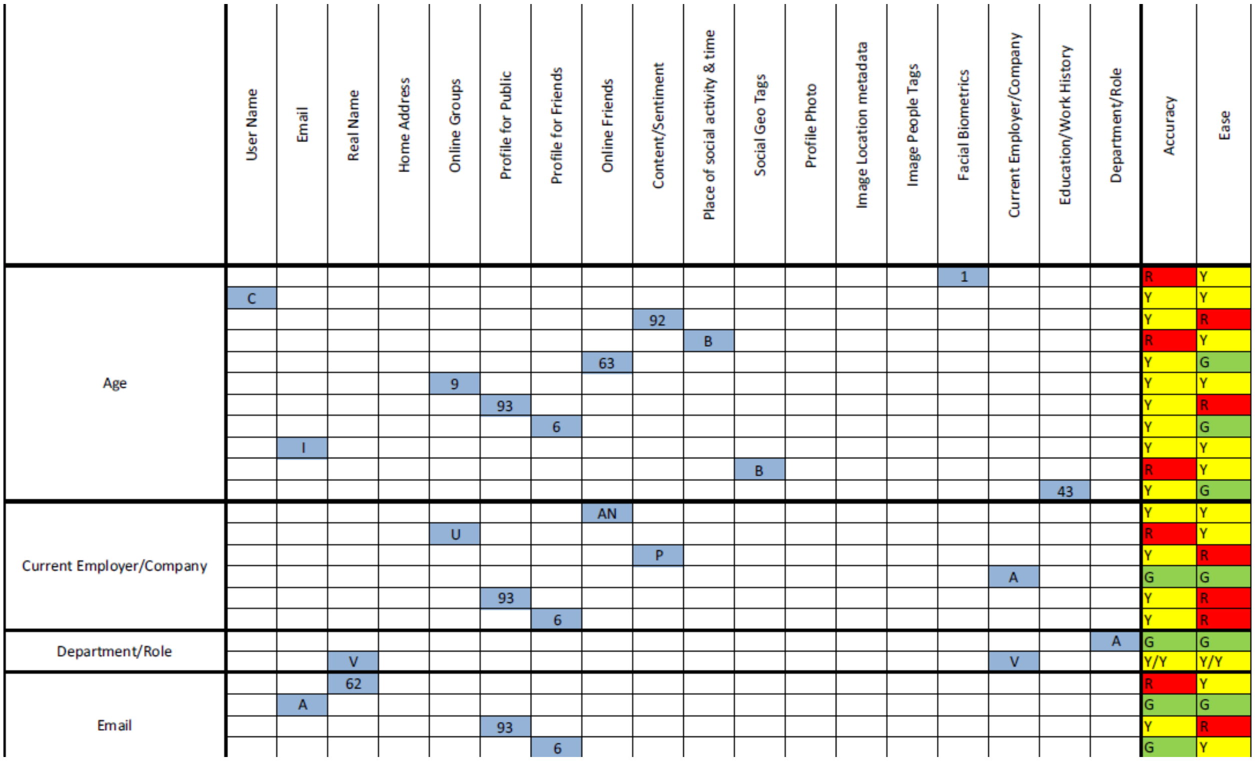
So [5] formulates some hypotheses which talk about the impact of notices and privacy threat awareness having a positive impact on online consumers ability to treat risks in terms of acceptance, mitigation and avoidance. The sample used for their study consisted of university students pursuing a major in information assurance. Hence, they had some varying levels of technical adeptness. They were asked to complete a survey which aimed to assess their awareness about various measures such as notices, risk awareness and risk management. A point to be noted here is that these students were educated about factors such as information which can link to a person's identity as well as data aggregation methods that make this linkage possible. This manipulation of the sample population would have had a bearing on the results as ordinary Internet users are not expected to have this knowledge. The participants were aged between 20 and 45 years old. However, most of the sample fell in between the ages of 20 and 24. So once, again the sample lacked diversity with respect to age groups and no information was provided in the paper with regard to any diversity existing in the population's ethnicity.

Results supported only three of the six hypotheses formulated by the researchers. The two hypotheses which proposed that the notice pertaining to an online entity's information privacy practices would end up positively affecting consumer to take up actions associated with risk mitigation and avoidance were not supported. Hence, the existence of a notice is not sufficient for an online consumer to manage privacy risks. In other words, control over the release of information is not the sole criteria for ensuring online privacy as it distracts users about the potential risks associated with divulgence of information. However, notice did have a positive impact on consumer actions with regard to accepting the risks associated with online privacy. The researchers speculate the cause for this would be owing to notices creating a sense of assurance about the safety of the user's information which is analogous to Brandimarte *et al*'s notion of giving them a sense of perceived control over its release. Therefore, even a false sense of assurance that can be mapped to a false sense of control may lead to the implicit acceptance of the risks involved with dealing with an online entity. Another finding was that the hypothesis which proposed that if consumers were aware about the privacy threats pertaining to an online entity's consumer information practices, then this would end up positively influencing their actions with respect to risk mitigation and avoidance was supported. Moreover, the hypothesis which stated that if consumers were more aware about the privacy threats pertaining to an online entity's consumer information practices, then they would be less likely to choose acceptance of the risk was also supported. A possible explanation drawn out by the researchers for this trend was that awareness about privacy risk would make use users more cautious thereby resulting in a negative impact on its acceptance.

In a nutshell, this study pointed out that notice and awareness about privacy are two distinct concepts. Awareness about risks associated with disclosure of information online is a must to help users better safeguard their privacy. Moreover, their findings do indicate that threat awareness leads to consumers being more pro active with respect to risk treatment in terms of avoidance and mitigation as well as exercising a greater sense of caution by not accepting the risk. Therefore, these findings can strongly be connected to the problem in [2] where students accept the risks i.e. are willing to disclose information when they have a sense of assurance (or control) over its disclosure while overlooking the associated risks.

As I mentioned earlier, the sample was educated with regard to what the survey was about. Some of them also claimed to have some levels of technical adeptness which exceeded normal Internet users. These factors would have had some bearing on the results. Moreover, this sample was not representative as it mostly consisted of people aged between 20 and 24 years old and was confined to students who had some technical background. Since, most of the participant's ages were within the same age groups as the participants in [2], I can assume that risk awareness can definitely have a positive impact on people within this age range. However, it is too early to say that this is a "one-size fits all solution" since a more representative sample would be needed to validate this.

A study done by Creese *et al* [3], talks about making online privacy risks more tangible to users of social networking websites. This is facilitated by means of a data-reachability model that is encoded in the form of a matrix. This model is used to elucidate privacy related information associated with the use of Online Social Networks (OSNs). The authors of this work point out that if attackers are provided with an initial dataset pertaining to a few attributes of ONS users, then they are potentially capable of aggregating this data to derive a vast amount of identity specific data. The matrix attempts to capture this data as it potentially paves the way for greater online privacy risks. The matrix model also attempts to predict the ease and accuracy associated with attackers managing to pull this off. A snapshot of this model is illustrated in figure 1. Moreover, the researchers of this work hold the view that the information contained in the matrix is interesting enough to be deemed as a "missing piece in the puzzle" that makes online privacy risks more tangible to OSN users. Therefore, the authors propose to build a website with a user-friendly interface to display the information contained in the matrix. However, they overlook the cultural differences that might exist in terms of what privacy means to people of different cultures or ethnic origins [6]. Also another issue would be that users would never really be interested in knowing the implications of the data which the matrix contains and hence, possibly refrain from taking up measures to reduce potential security risks.



	User Name	Email	Real Name	Home Address	Online Groups	Profile for Public	Profile for Friends	Online Friends	Content/Sentiment	Place of social activity & time	Social Geo Tags	Profile Photo	Image Location metadata	Image People Tags	Facial Biometrics	Current Employer/Company	Education/Work History	Department/Role	Accuracy	Ease
Age															1				R	Y
	C																		Y	Y
									92										Y	R
										B									R	Y
								63											Y	G
					9														Y	Y
						93													Y	R
							6												Y	G
		I																	Y	Y
											B								R	Y
																	43		Y	G
Current Employer/Company								AN											Y	Y
					U														R	Y
									P										Y	R
																A			G	G
						93													Y	R
							6												Y	R
Department/Role																		A	G	G
			V													V			Y/Y	Y/Y
Email			62																R	Y
		A																	G	G
						93													Y	R
							6												G	Y

Figure 1. A part of the Data-Reachability Matrix (Creese *et al* [3])

4 The Inevitability of Self-Disclosure

According to the study carried out by Shin *et al.* [4], self-disclosure is another factor that needs to be considered in case of privacy related matters in online social networks. Self-disclosure refers to the disclosure of information about oneself and is delivered from person to person in a lingual form. At times it is a necessary prerequisite for a minimal communication link to be established with other parties. Hence, Shin *et al.* asserts that it is a must for users of Social Networking Websites to develop some relationships with other online entities (users and groups) if they have to make their presence felt with regard to networking with others via the Internet.

The purpose of their study was an attempt to infer if a correlation existed between the needs of self-disclosure and the privacy concerns of an individual making use of online social networking services. The findings concluded the opposite and hence, indicated that factors motivating self-disclosure and individual privacy concerns are two different concepts with respect to privacy in online social networks. The analysis pointed out that users in the study frequently ended up revealing some general information about themselves as well as information pertaining to education, family training, employment, habits and hobbies when using these social networks. However, their study did not note the level of granularity this information can have as social networking sites do have privacy filters to keep certain information public while some other information accessible to friends or exclusive to the users themselves.

The sample population which was analyzed for the study consisted of active users of social networking websites such as Cyworld, Facebook and Twitter. However, the study made no mention of the sample size as well as failed to impart any information about the cultural backgrounds of the participants. However, the authors did mention that their sample was not representative owing to lack of diversity as a limitation of their work.

5 Discussion

From my analysis it is evident that several parameters such as control, risk awareness and self-disclosure exist which influence the privacy requirements of Internet users. The popular thought prevalent among governments, industrial organizations and security policy makers with regard to safeguarding online privacy relies solely on granting more control to individuals [2]. If a solution has to exist to the problem pointed out by [2] then the above parameters have to be understood and effectively linked together. Moreover, other factors need to be considered such as demographics in terms of a subject's cultural background to get a better understanding about differences in privacy concerns in different cultures. Also there is a possibility that online privacy requirements might vary for people belonging to different age groups.

The question which I posed at the start can be answered by considering the factors discussed in this work. Firstly, control is a necessary albeit not a sufficient factor for online security policy makers to pay attention to. Policy makers should bear in mind that if more control is given to Internet users over the release of their information, some attention needs to be given to other parameters such as the immediate consequences (threats to privacy) that would arise if this information was divulged. The notion of increased control would distract users about the risks involved in disclosing information. However, users would not care much about these risks in case of Social Networking Websites as they are not bothered about disclosing information associated with their family, employment, education and habits in addition to some general information about themselves [4]. This notion of self-disclosure might be a must if they have to network with other users on these websites. Another motivating factor for users of social networking websites being less concerned over the security of their personal information could be due to some craving for publicity.

But this whole idea would change in case of a setting discussed by [5] which deals with online shopping. In this case online consumers need to have some awareness about the risks involved especially in case of information which might potentially result in their identification while performing online dealings. This might result in issues such as identity thefts or illicit use and manipulation of an individual's personal information. This may lead to personal losses. For instance, if an individual's credit card information or online banking account password gets compromised due to the owner carelessly disclosing it to some shady entity online, then this would lead to financial losses and even debts. Hence, the context of a user's Internet usage also needs to be taken into account as far as understanding online privacy requirements is concerned.

6 Conclusion and Future Work

This report talked about different factors that should be taken into consideration while attempting to understand requirements associated with online privacy. It built up on the context of increased control resulting in a control paradox by analyzing other pieces of work in the existing literature which looked at different angles of online privacy. So what I could infer was that requirements for online privacy vary as per the context of a user's Internet usage i.e. in terms of social networking or performing some online transactions such as online shopping and online banking. The studies analyzed in the literature also pointed out that user awareness about potential threats to privacy in case of online shopping. This awareness would create a sense of caution among users with respect to revealing sensitive information while performing such transactions. My analysis did not consider studies which took into account diverse samples in terms of age groups and cultural diversity. This sets up a stage that motivates future research while taking the parameters of control, risk awareness and self-disclosure into account.

References

[1] Blase Ur and Yang Wang. 2013. A cross-cultural framework for protecting user privacy in online social media. In *Proceedings of the 22nd international conference on World Wide Web companion* (WWW '13 Companion). International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, Switzerland, 755-762.
Available url: http://delivery.acm.org.ezproxy.auckland.ac.nz/10.1145/2490000/2488037/p755-ur.pdf?ip=130.216.158.78&id=2488037&acc=ACTIVE%20SERVICE&key=C2716FEBFA981EF170F24D6534951B0D7F576284B32AF9B7&CFID=255369412&CFTOKEN=84983511&__acm__=1382352883_8a1955458e91448d1dc5cfcab734770c

[2] Brandimarte, Laura, Alessandro Acquisti, and George Loewenstein. "Misplaced Confidences Privacy and the Control Paradox." *Social Psychological and Personality Science* 4.3 (2013): 340-347.
Available Url: http://spp.sagepub.com.ezproxy.auckland.ac.nz/content/4/3/340.short

[3] S. Creese, M. Goldsmith, J. Nurse, and E. Phillips, “A data-reachability model for elucidating privacy and security risks related to the use of online social networks," in 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2012, pp. 1124-1131.
Available url: http://dx.doi.org.ezproxy.auckland.ac.nz/10.1109/TrustCom.2012.22

[4] Shin, S.; Yumi Ko; Jihwa Jang, "The conflict between privacy and self-disclosure in Social Networking Services," *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on*, vol., no., pp.490,493, 27-29 May 2011
doi: 10.1109/ICCSN.2011.6014772
Available url: http://ieeexplore.ieee.org.ezproxy.auckland.ac.nz/stamp/stamp.jsp?tp=&arnumber=6014772

[5] Spears, Janine L., "The Effects of Notice versus Awareness: An Empirical Examination of an Online Consumer's Privacy Risk Treatment," *System Sciences (HICSS), 2013 46th Hawaii International Conference on* , vol., no., pp.3229,3238, 7-10 Jan. 2013
doi: 10.1109/HICSS.2013.519
Available Url: http://ieeexplore.ieee.org.ezproxy.auckland.ac.nz/stamp/stamp.jsp?tp=&arnumber=6480233

[6] Xu, H., et al., Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. Journal of the Association for Information Systems, 2011. 12(12): pp. 798-824.
Available Url: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1595&context=jais