**Yeslam Al-Saggaf**
**Md Zahidul Islam**

# Privacy in Social Network Sites (SNS): The threats from data mining

***This paper explores the potential of data mining as a technique that could be used by malicious data miners to threaten the privacy of SNS users and makes a moral case for the users' right to privacy. It applies a data mining algorithm to a hypothetical dataset of a sample of individuals from Saudi Arabia, Pakistan and Yemen to show the ease at which characteristics about the SNS users can be discovered and used in a way that could invade their privacy. It is hoped by exploring the threats from data mining on individuals' privacy and arguing for users' right to privacy, the study will raise SNS users' awareness about the ways in which information that they reveal online can be used by malevolent data miners to harm them and how to operate in SNS safely***

**Keywords: privacy, Social Network Sites (SNS), data mining**

## Introduction: SNS and Facebook

Social Network Sites (SNS) continue to be among the most popular websites on the internet. According to most recent rankings from Alexa (2011a) of the top 500 sites, Facebook is ranked second from the top (in terms of the total number of page views) followed by YouTube in third place, Blogger in the seventh and Twitter in the tenth; suggesting that social networking is one of the popular internet activities among the two billion world internet citizens (Internet World Stats 2011). There are many SNS on the web including MySpace, Twitter, Hi5, Flickr, Orkut, LinkedIn and BeBo, but by far Facebook is the most popular site (Alexa 2011a). Indeed, this observation is consistent with Facebook statistics that showed in less than a year, the number of active users on Facebook has jumped from 500 million to 800 million users, 50 per cent of whom log on to it each day (Facebok 2011). This massive growth in the population size of Facbook is indicative of the huge popularity that Facebook enjoys.

There are not many definitions of SNS in the literature (Al-Saggaf 2011), but the most frequently cited definition is the one proposed by Boyd and Ellison (2007: 211) who defined SNS as web-based services that allow individuals to:

1) construct a public or semi-public profile within a bounded system;
2) articulate a list of other users with whom they share a connection, and
3) view and traverse their list of connections and those made by others within the system.

This definition is not just chosen because it is the most frequently used one but also because it incorporates most of the elements found on Facebook such as being a platform where individuals can communicate with each other to form new social connections and/or to maintain existing friendships and in doing so share personal information, photos, videos, thoughts as well as their feelings. This view about Facebook is in line with the results from a recent study which has shown that people use SNS not only to develop new friendships but also to communicate with older friends whom they cannot meet regularly face-to-face (Al-Saggaf 2011). In addition, Facebook allows its members to communicate with others using voice, videos, online chat, offline messages, blogs and 'walling'[1] (Al-Saggaf 2011).

Upon registering with Facebook, the first thing users do is create their own profiles, which they can set to be either private or public. Like any other SNS, Facebook allows its users to upload their photos, videos and emotional states. The site also allows outside developers to build applications which users can then use to personalise their profiles and perform other tasks, such as comparing movie preferences and charting travel histories (Boyd and Ellison 2007). In addition, users can also create their own online identities (Jones et al 2008). To create their identities on SNS, users need to place on their own profiles their personal and biographical data such as name (a real name or alias), date and place of birth, citizenship, nationality, photos, hobbies, and so on.

While on the one hand users are increasingly aware and very concerned about their privacy on Facebook (Boyd and Ellison 2007, Jones et al 2008, Young 2009, Al-Saggaf 2011), on the other hand, self-disclosure and revealing private information on the site is very widespread (Jones et al 2008, Valenzuela, Park and Kee 2009, Al-Saggaf 2011) with users sharing with strangers up-to-the-minute updates of the status of their feelings and thoughts. Given young adults between the ages of 18-24 represent the largest cohort of SNS users (Hoy & Milne 2010), revealing private information such as political views, residential address, date of birth, books read, movies watched, schools went to, sexual orientations and their inner thoughts about their partners, neighbours, colleagues and employers can have serious consequences for these users' informational privacy and possibly also for their financial and physical security.

This paper explores the potential of data mining as a technique that could be used by malicious data miners to threaten the privacy of SNS users and makes a moral case for the protection of users' privacy. By exploring threats from data mining to individuals' privacy and arguing for users' right to their privacy, the study will raise SNS users' awareness about the ways in which information that they reveal online can be used by malevolent data miners to harm them. To achieve this aim, a hypothetical dataset of a sample of individuals from Saudi Arabia, Pakistan and Yemen, as examples of conservative societies, was created. Next, the paper applied a data mining algorithm to this dataset to demonstrate the ease at which characteristics about the SNS users can be discovered and used in a way that could invade their privacy. After that the paper will present a short philosophical analysis to argue for the importance of protecting users' privacy from the threats of data mining. At the end, we will present several recommendations that should contribute to raising users' awareness about how to operate in SNS safely.

**Privacy as an ethical issue**

Privacy on Facebook can be threatened in many ways including through the continuous changing of the privacy settings that Facebook does without announcing to users, tracking technologies such as HTTP cookies that gather information about users without their knowledge and Application Programming Interface (API) tools that enable other SNS to share users' information and create complete profiles enabling them, in essence, to sell this information to third parties. Another method that can be used to erode users' privacy is data mining. When a data mining algorithm is applied to a large dataset which can be created by harvesting users' information from SNS, hidden and non-obvious patterns about those users can be unearthed from this dataset (Tavani 2011). Used unethically on Facebook users, data mining can have the potential of incorrectly placing users in newly created categories or groups that could, for example, make them victims of paedophiles or organised crime.

Privacy is one of the most widely discussed topics in the Australian media and in the computer and information technology ethics literature (Al-Saggaf and Weckert 2011). But what is privacy? What is considered as private? And why is privacy valued anyway? There are three theories of privacy (Tavani 2011). The first theory relates to the notion of Accessibility Privacy, which defines privacy in terms of one's physically 'being let alone' or freedom from intrusion into one's physical space. The second theory relates to Decisional Privacy, which defines privacy in terms of freedom from interference in one's choices and decisions. The third, and most relevant theory to this article, is that of Informational Privacy, which defines privacy as control over the flow of one's personal information, including the transfer and exchange of that information (Tavani 2011: 137). In addition, Moor (2000 cited in Tavani 2011) has also introduced an account of privacy that is more comprehensive in that it encapsulates all these three theories. Specifically, it incorporates the elements of the non-intrusion, non-interference and informational views of privacy.

According to Moor, an 'individual has privacy in a situation if in that particular situation the individual is protected from intrusion, interference, and information access by others' (ibid: 137). Tavani also notes that Moor makes a distinction between naturally private and normatively private situations. According to Tavani (ibid), this distinction allows us to distinguish between the conditions required for having privacy (in a descriptive sense) and having a right to privacy in the normative sense. According to this distinction, if a person sees another picking her nose in the library, then that person lost her privacy but her privacy was not violated. But if that other person peeps through the keyhole of her apartment door then her privacy is not only lost but also violated.

What is normally considered to be private? This question has also been raised by Weckert and Adeney (1997) and their answer is that our inner thoughts, our personal relationships, and our personal information such as those relating to our health and finances are all private matters. Informational privacy is seen in different ways. For example, Islam (2008) and Islam and Bronkovic (2011) consider the exact information on any attribute of an individual (such as the disease diagnosis of a patient and income of an employee) as private while Murahidhar et al. (1999) consider any exact information about a group of individuals as private even if it is not clear which individual the disclosed information belongs to.

Privacy is valued for many reasons including for achieving important human ends like trust and friendships (Tavani 2011). For Jim Moor (2004, cited in Tavani 2011), privacy is important because it is the articulation or expression of the core value of security (ibid). On the other hand, for Deborah Johnson privacy is an important social good because when people are watched all the time they take the perspective of the observer. Because decisions will be made on the basis of what they do, they tend to think before acting. This becomes a form of social control which leads to eroding individuals' freedom. This in turn affects democracy (Johnson 2001). In our view, privacy is also important for love, marriage and partner relationships, respect and dignity, freedom of expression and liberty, autonomy, solitude, anonymity and secrecy, data protection and self-confidence to name a few.

Erosion of privacy due to excessive self-disclosure is a problem for participants in SNS and users are more than ever concerned about their privacy (Boyd and Ellison 2007, Jones et al 2008, Young 2009, Al-Saggaf 2011). That said, self-disclosure is rampant on both SNS (Jones et al 2008, Valenzuela, Park and Kee 2009) and online communities (Dyson 1998, Horn 1998, Kollock and Smith 1999, Markham 1998, Rheingold 2000). There are many reasons for this but the lack of oral and non-verbal cues, and lack of public self-awareness are major factors. Lack of oral and non-verbal cues, and lack of public self-awareness cause abandonment of social inhibitions and detachments from social conventions (Barnes 2001, Joinson 1998, Mar 2000, Preece 2000, Rafaeli and Sudweeks 1997, Wallace 1999).

Trust between online communicators has been found to be another factor that encourages self-disclosure (Valenzuela, Park and Kee 2009). Trust is vital for personal relationships (Cocking and Matthews 2000, Weckert 2003); in fact, one way to show the strength of a friendship between two individuals is by demonstrating they trust each other. At the same time to show my trust in someone I have to reveal more about myself. That is why self-disclosure is also important for personal relationships (Preece 2000, Rheingold 2000, Rifkin 2000, Wallace 1999). Indeed, researchers have found that as people become familiar with others online, they tend to reveal more about themselves (Barnes 2001, Horn 1998, Markham 1998).

But, as online communicators reveal more and more sensitive information about themselves, the chances that their privacy will be eroded or, at least, violated will be increased. For example, women in Saudi Arabia who place their photos (even the ones that show their faces) on Facebook may become subject to sexual coercion by malicious SNS users if these photos fall into these malicious SNS users' hands. They could threaten to release their photos or video clips on the internet or publicly via Bluetooth on mobile phones unless these women submit to their demands. If the women do not comply, the result can cause serious damage to their family's reputation which is a grave matter in Saudi society. While this example suggests that privacy is not valued equally in all cultures (placing photos on Facebook may not be an issue for women in Western societies), it nevertheless shows that privacy has at least some value in all societies (Tavani 2011).

**Data mining threats to the privacy of users of Facebook and/or other SNS**

There are various data mining tasks including data collection (such as automatic collection of weather data from different sensors), data pre-processing (such as pre-processing of satellite images), data integration/transformation to prepare a suitable flat file containing a range of relevant non-class attributes (such as blood sugar level and cholesterol level of a patient) and a class attribute (such as diagnosis of disease), data cleansing (by identifying and removing/correcting corrupt data, and imputing missing values), and pattern extraction from the clean pre-processed data (Islam 2012). There are a number of pattern extraction techniques including clustering (such as K-means and Fuzzy C-means clustering), classification (such as decision trees and artificial neural networks) and association rule mining such as finding purchase patterns from a market basket dataset.

Data mining has a wide range of applications such as social network analysis, analysis of microarray gene expression data, software engineering, market segmentation, web search result grouping, and irrigation water demand forecasting – just to name a few (Zhao and Zhang 2011; Haung and Pan 2006; Lung, Zaman, and Nandi 2003; Tsai and Chiu 2004; Zamir and Etzioni 1999). Data pre-processing techniques can be applied to collect data from various sources including weather stations, satellite images and water usage statements. Various other data mining techniques (such as classification by decision tree and artificial neural network) can then be applied on the collected data to extract patterns that can then be used to predict future water demand for irrigation. Accurate water demand prediction can help us to manage irrigation water more efficiently by reducing the wastage of already limited irrigation water. Data mining can also be applied on huge amounts of data generated from social networking sites (SNS) in order to study contact networks, growth rates and social implications of various SNS (Patton 2007).

Data mining is also used in direct marketing (where targeted advertisements are sent to potential customers), and various business analyses. An example of its application in developing better business strategies and business promotion is association rule mining (Islam 2008). Association rule mining is applied on a huge set of transactions (records), where each transaction consists of a list of items such as milk, bread, butter that are sold together in the transaction. A supermarket chain, for example Wal-Mart, collects each and every sale transaction in a central data warehouse from all its stores (around 2900) situated in around six different countries. From the collected data, they can explore frequent item sets and association rules. When a set of items appear in a huge number of transactions then they are known as a frequent item set. Moreover, when the appearance of one set of items in a transaction increases the possibility of the appearance of another set of items in the same transaction then it is known as association rule. Based on frequent item sets and association rules a supermarket can design its store in order to increase sales. For example, they can put the frequent items apart in a store so that customers need to walk through the store to find the items. This can often increase the sales as customers tend to buy more items when they walk through them. Moreover, supermarkets can reduce the prices of a set of items and advertise the price reduction. However, they can increase the prices of another set of items when they know from association rule mining that the increased sale of the former set of items will also increase the sales of the later sets of items and therefore, they will make more overall profit.

Data mining can extract various interesting and hidden patterns (such as logic rules and clusters) from a dataset. Often it is argued that general patterns (logic rules) are public knowledge and should be considered sensitive to individual privacy (Islam, 2008; Islam and Bronkovic, 2011). For example, the pattern that people from Asia have black hair is public knowledge and therefore should not be considered sensitive. If a person is originally from Asia then it is generally assumed that he/she has black hair and there is nothing wrong with that. However, some general patterns even when they are applicable to many people can disadvantage an individual and therefore need to be considered as sensitive. For example, if a bank discovers that all previous loans granted to the customers living in a specific suburb are defaulted and, therefore, decides to turn down the loan application of an individual living in the suburb just based on his/her address then this pattern can appear to be unfair to the individual. Similarly, if a business learns from its past records that all employees of a race have been found inefficient and, therefore, decides not to offer a job to a new applicant who is from the same race, then the pattern can again appear to be unfair to the applicant.

Tavani (2011) presents an example of such intrusive and privacy threatening data mining where a car loan application, for purchasing a new BMW, was turned down by a bank although the applicant was financially solvent and had an executive position with good salary. The bank mines its data sets and discovers a pattern that executives earning between $120K and $150K annually, who often take expensive vacations and purchase luxury cars generally start their own businesses. The bank then mines another data set and finds that the majority of such entrepreneurs declare bankruptcy within a year. Unfortunately, the applicant for the car loan falls in this category, although neither the applicant nor the bank knows whether the applicant will really start his own business and face bankruptcy in future.

Data mining can be used for extracting various sensitive patterns of activity by the Facebook or other SNS users. The patterns can then be applied on any Facebook (or any other SNS) user resulting in huge user discomfort and serious breach of individual privacy. For example, a malicious data miner can study the Facebook activities of his/her friends. Based on the observation he/she can then prepare a dataset (a table with records and attributes) having information on the users. In the dataset each record can represent a Facebook user and each column/attribute can represent a property of the user. The properties can be learnt from the Facebook use patterns. Examples of the attributes can include: 'Ratio of the number of opposite sex friends to same sex friends' (Col. 6 in Table 1), 'Number of own picture uploads per week' (Col. 3 in Table 1), 'Level of exposure of the pictures (i.e. how exposed the person is in the pictures)' (Col. 4 in Table 1), and 'Number of status changes in Facebook per week' (Col. 5 in Table 1).

The data miner can have some supplementary knowledge on his/her friends in addition to the knowledge learned from their Facebook activities. The data miner can also use the supplementary knowledge to create a class attribute of the dataset. The class attribute can be considered as the label of a record. All other attributes are considered as non-class attributes. Classification task (using techniques including decision tree and artificial neural network) builds logic rules from the dataset to classify the records on the values of the class attribute. An example of a logic rule can be 'if A = $a_1$ and B = $b_1$ then C = $c_1$' where A and B are non-class attributes, C is the class attribute and $a_1$, $b_1$, $c_1$ are the attribute values.

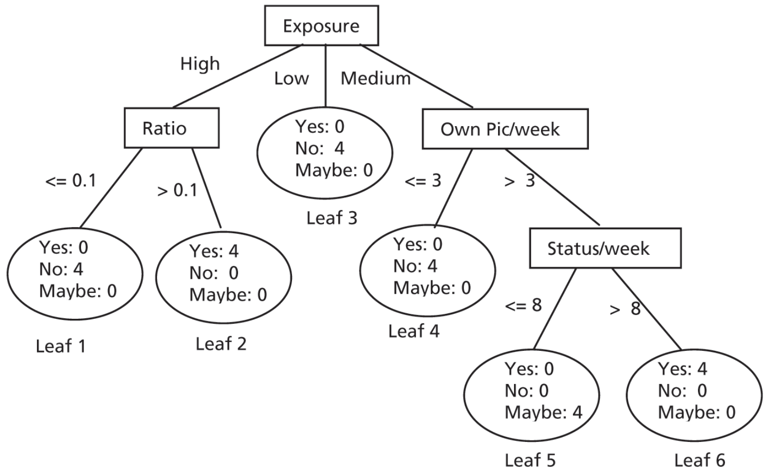
Based on his/her supplementary knowledge on each friend in the Facebook, a malicious data miner can add an attribute, say 'Willingness to date with a male' (Col. 7 in Table 1) as the class attribute having values 'yes', 'may be' and 'no' for the records of the dataset created from the Facebook observation. All other attributes can be considered as non-class attributes. The data miner can then apply a classifier on the dataset and extract sensitive logic rules to classify a Facebook user as either 'Willing to date with a male' or 'Not willing to date with a male'. Once the logic rules are built they can be used on any Facebook user (whom the data miner might not even know personally) to classify as either 'Willing to date with a male' or 'Not willing to date with a male' simply based on the users' Facebook activities. The malicious data miner can then approach the female users who fall in the category 'Willing to date with a male' for a date. This can be disturbing for a Facebook user especially in a conservative society. If a female Facebook user falls in the category 'Willing to date with a male' serious social problems can arise including extortion, difficulty in finding a partner and even inferior treatment in a job environment.

We now give a hypothetical dataset of a sample of individuals from Saudi Arabia, Pakistan and Yemen, as shown in Table 1, created from Facebook activities and supplementary knowledge of a malicious data miner.

**Table 1: A sample dataset of Facebook users**

| | | | | | | |
|---|---|---|---|---|---|---|
| 21 | Saudi | 7 | High | 3 | 0.1 | No |
| 19 | Pakistan | 2 | High | 2 | 4 | Yes |
| 33 | Yemen | 7 | High | 2 | 4 | Yes |
| 35 | Saudi | 2 | High | 7 | 0.1 | No |
| 19 | Pakistan | 2 | Medium | 12 | 3 | No |
| 25 | Yemen | 3 | Medium | 3 | 4 | No |
| 22 | Saudi | 7 | Medium | 7 | 0.1 | Maybe |
| 33 | Pakistan | 8 | Medium | 8 | 5 | May be |
| 21 | Saudi | 7 | Medium | 22 | 5 | Yes |
| 27 | Saudi | 8 | Medium | 33 | 1 | Yes |
| 22 | Saudi | 2 | Low | 22 | 7 | No |
| 26 | Saudi | 8 | Low | 2 | 2 | No |
| 21 | Saudi | 7 | High | 3 | 0.1 | No |
| 19 | Pakistan | 2 | High | 2 | 4 | Yes |
| 33 | Yemen | 7 | High | 2 | 4 | Yes |
| 35 | Saudi | 2 | High | 7 | 0.1 | No |
| 19 | Pakistan | 2 | Medium | 12 | 3 | No |
| 25 | Yemen | 3 | Medium | 3 | 4 | No |
| 22 | Saudi | 7 | Medium | 7 | 0.1 | Maybe |
| 33 | Pakistan | 8 | Medium | 8 | 5 | Maybe |
| 21 | Saudi | 7 | Medium | 22 | 5 | Yes |
| 27 | Saudi | 8 | Medium | 33 | 1 | Yes |
| 22 | Saudi | 2 | Low | 22 | 7 | No |
| 26 | Saudi | 8 | Low | 2 | 2 | No |

A data miner can apply a decision tree algorithm (for example, C4.5) on the training dataset shown in Table 1 and build a decision tree as shown below that considers 'Willingness' as the class attribute. The rectangles denote internal nodes and the ovals denote leaves of the tree. There are six leaves and four nodes in the tree. Each leaf of the tree represents a logic rule that classifies the records belonging to the leaf. For example, the logic rule for Leaf 1 is 'If exposure = high, and ratio <= 0.1 then willingness = no'. There are four records belonging to the leaf meaning that four records have 'Exposure = high and ratio <= 0.1' in the training dataset shown in Table 1. In this example, out of the four records all of them have 'Willingness = no'. Therefore, Logic Rule 1 suggests that if a Facebook user uploads pictures with high exposure and the ratio of male friends to female friends is less than or equal to 0.1 then she is usually not willing to date a male. However, Logic Rule 2 (for Leaf 2) suggests that if picture exposure of a Facebook user is high and ratio of male to female friends is greater than 0.1 then she is likely to be willing to date a male since out of four such records in the training dataset all are willing to date a male. Similarly, Leaf 5 and Leaf 6 also represent logic rules that classify records as willing to date.



A malicious data miner can then use the knowledge on any other Facebook users whom he/she even does not know. The data miner can learn about the Facebook activities of a user through common friends. Therefore, the data miner may identify a Facebook user as willing to date even though he/she does not know the user. If the logic rules that label a user as willing to date are made public then anyone knowing the rules may classify a user as either willing or not willing to date. This can cause serious social and emotional trouble for the Facebook users who fall in the category of willing to date especially in conservative societies such as in Saudi Arabia, Yemen and Pakistan. This is especially more undesirable for those who are not willing to date but are approached by unwanted people. The logic rules are extracted using data mining algorithms from a sample training dataset and cannot guarantee a correct classification for a new record.

**The applicability of the study findings to Western societies**

The situation in Western countries is not as striking in many respects. However, the threats of data mining to privacy, highlighted above, are certainly not of concern to the above three conservative societies only. While, on the one hand, the younger generation in Western societies, as this paper has shown, has a greater tendency to have their profiles publicly available, on the other, they are also concerned about sharing personal information on Facebook and about their privacy. Similarly, while the risks associated with the application of data mining techniques on Facebook data to Western societies may be different than the risks to the above three conservative societies, they are certainly not less concerning. Consider the ability of data mining to place users in newly created categories or groups that could make them victims of crimes such as child pedophilia, child pornography, cyberstalking, cyberbullying, child sexual exploitation and child grooming.

A recent report published by the Australian Institute of Criminology shows online child grooming for sexual offences, for example, is already on the rise in Australia, the UK and the United States because of the misuse of SNS.[2] Data mining of SNS data could further exacerbate this crime which is taken very seriously in Western societies as the damage caused can be enormous and long lasting. So while the risks are different depending on the society one lives in, the harms that can be caused by data mining are no less important.

**A moral case for the SNS users' right to privacy**

The section titled 'Privacy as an ethical issue' above discussed some specific reasons why privacy is valued. The aim of this section is to make a moral case for the SNS users' right to privacy using both utilitarianism and deontology ethical theories. From a utilitarian perspective, it would appear that using data mining to invade SNS users' privacy can harm them. For example, malicious SNS users can use data mining technologies to target women on Facebook and threaten them to either submit to their sexual desires or face the consequences of having hidden but sensitive information about them posted on the internet or distributed publicly, thereby damaging their family reputation. Putting restrictions on the use of data mining (more on this below) can certainly help stop harm from being inflicted upon those women. This shows that data mining can be used to cause harm to people but that privacy can protect individuals from these kinds of harm.

From a deontological perspective it would appear developers of data mining algorithms have a duty of care to the people who are likely to be affected by the algorithms they develop. While it may be difficult to ensure that these value laden technologies cannot be used by malicious data miners to invade people's privacy, developers of data mining algorithms have a responsibility also to develop privacy preserving techniques. Respect for persons entails that people should be treated as ends in themselves, and not just as means to some end. To treat SNS users with respect means they should be treated as persons who have value in themselves, and not only as pieces of information that could be useful, for example, to third party advertisers. SNS owners should exercise caution when selling/sharing their users' data to/with third party advertisers. So a dataset from users' data should not be made available to malicious data miners to mine and use the results against the vulnerable and unsuspecting members of the society and thus breach their privacy.

Privacy protects some freedoms and restricts others. It protects an individual's freedom to be alone, to act without others intruding and to control what others know about him or her. However, it restricts the extent to which an individual can observe others and what he or she can learn about others (Weckert and Adeney 1997); although in the case of the SNS, much to the dismay of the users, this may not be possible. That is, privacy may not be able to restrict the freedom of the malicious SNS users to use data mining algorithms to uncover hidden information about a few people with the mission to target them individually because SNS users' data (necessary for the dataset) and data mining algorithms can easily be acquired. This suggests that privacy in this case may not, when it should, restrict the freedom of the malicious SNS users to harm others. Thus, while it might be argued that the moral value of privacy comes from its specific function in promoting the liberty of individuals by restricting the scope of the power of those in positions of strength (data miners), in the case of these SNS users, this may not happen (Weckert and Adeney 1997).

But why should the SNS users be concerned about their privacy? The number of times they update their status a week or the level of exposure within the photos they share, for example, are the business of nobody except these SNS users but is this information in itself important to the SNS users? Weckert and Adeney (1997) argue that their preference for unsugared, black coffee rather than the sweet, white variety is also the business of nobody but them and the person making their coffee, but, according to them, worrying about the privacy of this information seems a bit extreme. While much information about the SNS users, like their age, gender, nationality and marital status, which some display on their SNS profiles, might not be much more important than the preference in coffee, the number of times they update their status a week or the level of exposure within the photos they share can reveal a little more about these users when information from other users is also added to the dataset and mined.

### Conclusion and recommendations to mitigate the risk

This article explored the potential of data mining as a technique that could be used by malicious data miners to threaten the privacy of SNS users and made a moral case for the protection of users' privacy. Using a hypothetical dataset of a sample of individuals from Saudi Arabia, Pakistan and Yemen, a data mining algorithm was applied to this dataset to demonstrate the ease at which characteristics about the SNS users can be discovered and used in a way that could invade their privacy. This was followed by a short philosophical analysis which argued for the importance of protecting users' privacy from the threats of data mining.

Privacy is a crucial social good and an instrumental, if not intrinsic, universal value (for the difference between instrumental and intrinsic values see Burmeister, Weckert and Williamson 2011). Privacy is valued for many reasons (as discussed above). While people generally learn about privacy and how to maintain it from their parents, schools and society, the development of technologies has meant that people are operating in environments that did not exist in the past. As a result, on the one hand, people are facing new challenges, on the other hand, they do not seem to get clear guidelines from their parents, schools, and society on how to operate safely in these new environments such as SNS.

Privacy is often not taken seriously by many users especially the young users group. It is essential for SNS users to be careful in maintaining their privacy online for reasons discussed above. Therefore, it is important to raise their awareness about the possible privacy invasions and their implications. One way to preserve privacy online is by masking the individual's data carefully or hiding the sensitive information such as date of birth, address and other identifying information. This way, even if an unknown malicious data miner can classify a user, for example, as 'Willing to date', it can be difficult for the miner to locate the user and thus harass her. At the same time, if the logic rules are known to the users they can deliberately design their activities in a way so that she is not classified as 'Willing to date'. For example, if the exposure of a user is 'medium' in her pictures then she can deliberately keep the number of her own picture uploads per week less than three so that she falls in Leaf 4 and thereby safely classified as 'Not willing to date'.

Another way to protect privacy online is by putting restrictions, possibly in the form of laws and regulations, on the use of data mining for individual purposes. However, restricting malicious data mining by introducing laws can be a difficult job. First it will be difficult to detect that someone is mining data maliciously. Second, even if detection is possible it will be difficult to prove malicious intent. One can always argue that he/she was performing data mining for good intentions such as research and knowledge discovery.

We therefore recommend that the data mining community should develop Privacy Preserving Data Mining (PPDM) techniques specifically catered for online environments. Until such techniques are developed, users should protect themselves by using all possible ways including hiding their identifying information, using SNS privacy settings carefully and masking their online activities to protect them from being identified as potential victims. Ensuring the privacy settings on Facebook are up to date (often they roll back to the default settings) can be another way to keep malicious data miners out of the way.

The threats from data mining on individuals' privacy are serious as the application of a data mining algorithm on the above dataset has shown; and users should have a right to their privacy online as the short philosophical analysis has shown. While the recommendations offered here do not solve the problems, it is hoped the paper has at least begun to raise SNS users' awareness about the ways in which information they reveal online can be used by malevolent data miners to harm them and how to operate in SNS safely in the midst of these threats.

## Notes

[1] The participants in Al-Saggaf's (2011) study call the activity of posting comments and other objects on their Facebook wall to communicate with their friends as 'walling'

[2] See http://www.aic.gov.au/en/publications/current%20series/rpp/100-120/rpp103.aspx, accessed on 21 November 2011

## References

Alexa (2011a) The top 500 sites on the web. Available online at http://www.alexa.com/topsites, accessed on 21 November 2011

Alexa (2011b) The top 500 sites on the web. Available online at http://www.alexa.com/topsites/countries/SA, accessed on 21 November 2011

Al-Saggaf, Y. (2003) Online communities in Saudi Arabia: An ethnographic study, PhD thesis, Charles Sturt University, Wagga Wagga, Australia

Al-Saggaf, Y. (2006) The online public sphere in the Arab world: The war in Iraq on the Al Arabiya website, *Journal of Computer-Mediated Communication*, Vol. 12, No. 1. Available online at http://jcmc.indiana.edu/vol12/issue1/al-saggaf.html, accessed on 15 April 2008

Al-Saggaf, Y. (2011) Saudi females on Facebook: An ethnographic study, *International Journal of Emerging Technologies and Society*, Vol. 9, No. 1 pp 1-19

Al-Saggaf, Y. and Weckert, J. (2011) Privacy from a Saudi Arabian perspective, *Journal of Information Ethics*, Vol. 20, No. 1 pp 34-53

Barnes, S. B. (2001) *Online connections: Internet interpersonal relationships*, Hampton Press, New Jersey

Bastani, S. (2000) Muslim women on-line, *Arab World Geographer*, Vol. 3, No 1 pp 40-59

Burmeister, O. K., Weckert, J. and Williamson, K. (2011) Seniors extend understanding of what constitutes universal values, *Journal of Information, Communication and Ethics in Society*, Vol. 9, No. 4. pp 238-252

Boyd, D. M. (2006) Friends, friendsters, and Top 8: Writing community into being on social network sites, *First Monday*, Vol. 11, No. 12. Available online at http://www.firstmonday.org/issues/issue11_12/boyd, accessed on 12 October 2009

Boyd, D. M. and Ellison, N. B. (2007) Social network sites: Definition, history, and scholarship, *Journal of Computer-Mediated Communication*, Vol. 13, No. 1. Available online at http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html, accessed on 15 April 2008

Cocking, D. and Matthews, S. (2000) Unreal friends*, Ethics and Information Technology*, Vol. 2 pp 223-231

Dyson, E. (1998) *Release 2.1: A design for living in the digital age*, Broadway Books, New York

Emerson, D. (2008) Facebook friends not real friends: judge, *Sydney Morning Herald*. Available online at http://www.smh.com.au/news/technology/facebook-friends-not-real-judge/2008/03/27/1206207279597.html, accessed on 6 October 2009

Facebook (2011) Statistics. Available online at http://www.facebook.com/press/info.php?statistics, accessed on 21 November 2011

Fule, P. and Roddick, J. F. (2004) Detecting privacy and ethical sensitivity in data mining results. Paper presented to the 27th Australian Computer Science Conference (ACSC2004), Vol. 26 of Conference in Research and Practice in Information Technology, Estivill-Castro, Vladimir (ed.) pp 163-168

Garton, L., Haythornthwaite, C. and Wellman, B. (1997) Studying online social networks, *Journal of Computer-Mediated Communication*, Vol. 3, No. 1. Available online at http://jcmc.indiana.edu/vol3/issue1/garton.html, accessed on 18 September 2012

Hamman, R. (2001) Computer networks linking network communities, Werry, C. and Mowbray, M. (eds) *Online communities: Commerce, community action, and the virtual university*, Hewlett-Packard, New Jersey pp 71-95

Hauben, M. and Hauben, R. (1997) *Netizens: On the history and impact of usenet and the internet*, IEE Computer Society Press, Washington

Haythornthwaite, C. and Wellman, B. (2002) The internet in everyday life: An introduction, *The Internet in Everyday Life*, Wellman, B. and Haythornthwaite, C. (eds) Blackwell Publishers, Oxford pp 1-55

Horn, S. (1998) *Cyberville: Clicks, culture, and the creation of an online town*, Warner Books, New York

Huang, D., and Pan, W. (2006) Incorporating biological knowledge into distance-based clustering analysis of microarray gene expression data, *Bioinformatics*, Vol. 22 pp 1259-1268

Hoy, H.G and Milne, G. 2010. Gender differences in privacy-related measures for young adult Facebook users, *Journal of Interactive Advertising*, Vol. 10 pp 1525-2019

Internet World Stats (2011) Internet usage in the Middle East. Available online at http://www.Internetworldstats.com/stats.htm, accessed on 21 November 2011

Islam, M. Z. (2008) Privacy preservation in data mining through noise addition. PhD thesis in Computer Science, School of Electrical Engineering and Computer Science, the University of Newcastle, Australia

Islam, M. Z. (2012) Explore: A Novel Decision Tree Classification Algorithm, *Lecture Notes in Computer Science*, Vol. 6121 pp 55-71

Islam, M. Z. and Brankovic, L. (2011) Privacy preserving data mining: A noise addition framework using a novel clustering technique, *Knowledge-Based Systems*, December, Vol. 24, No. 8 pp 1214-1223

Johnson, D. G. (2001) *Computer ethics*, New Jersey, Prentice Hall, third edition

Joinson, A. (1998) Causes and implications of disinhibited behaviour on the internet, *Psychology and the Internet*, Gackenbach, J. (ed.), Academic Press, San Diego pp 43-60

Jones, S. G. (1998) Information, internet, and community: Notes toward an understanding of community in the information age, *CyberSociety 2.0: Revisiting Computer-Mediated Communication and Community*, Jones, S. G. (ed.), Sage Publications, Thousand Oaks, CA pp 1-35

Jones, S., Millermaier, S., Goya-Marthinez, M. and Schuler, J. (2008) Whose space is MySpace? A content analysis of MySpace profiles, *First Monday*, Vol. 13, No. 9. Available online at http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2202/2024, accessed on 18 September 2012

Karpinski, A. C. and Duberstein, A. (2009) A description of Facebook use and academic performance among undergraduate and graduate students, Technology Research Poster Session. Available online at http://researchnews.osu.edu/archive/facebook2009.jpg, accessed on 5 October 2009

Kollock, P. and Smith, M. (1999) Communities in cyberspace, *Communities in cyberspace*, Smith, M. and Kollock, P. (eds) Routledge, London pp 3-25

Lange, P. G. (2007) Publicly private and privately public: Social networking on YouTube, *Journal of Computer-Mediated Communication*, Vol. 13, No. 1. Available online at http://jcmc.indiana.edu/vol13/issue1/lange.html, accessed on 17 October 2009

Lung, C.-H., Zaman, M., and Nandi, A. (2004) Applications of clustering techniques to software partitioning, recovery and restructuring, *Journal of Systems and Software*, Vol. 73, pp 227-244

Mar, J. (2000) Online on time: The language of internet relay chat, Gibbs, D. and Krause, K. L. (eds) *Cyberlines: Languages and cultures of the internet*, James Nicholas Publishers, Australia pp 151-174

Markham, A. N. (1998) *Life online: Researching real experience in virtual space*, AltaMira Publications, Walnut Creek, CA

Mitra, A. (1997) Virtual commonality: Looking for India on the internet, Jones, S. G.(ed.) *Virtual culture: Identity and communication in cybersociety*, Sage Publications, London pp 55-79

Moor, J. (2000) Towards a theory of privacy for the information age, Baird, R. M., Ramsower, R. and Rosenbaum, S. E. (eds) *Cyberethics: Moral, social, and legal issues in the computer age*, Prometheus Books, New York pp 2000-2012

Moor, J. (2004) Reason, relativity, and responsibility in computer ethics, Spinello, R. and Tavani, H. T. (eds) *Readings in cyberethics*, Jones and Bartlett Publishers, Sudbury, MA, second edition pp 40-54

Muralidhar, K., Parsa, R., and Sarathy, R. (1999) A general additive data perturbation method for database security, *Management Science*, Vol. 45, No. 10 pp 1399-1415

Patton, S. (2007) Social Networking Sites: Data Mining and Investigative Techniques. Available online at https://www.blackhat.com/presentations/bh-usa-07/Patton/Whitepaper/bh-usa-07-patton-WP.pdf, accessed on 18 September 2012

Preece, J. (2000) *Online communities: Designing useability, supporting sociability*, John Wiley and Sons, Chichester

Rafaeli, S. and Sudweeks, F. (1997) Networked interactivity, *Journal of Computer-Mediated Communication*, Vol. 2, No. 4. Available online at http://jcmc.indiana.edu/vol2/issue4/rafaeli.sudweeks.html, accessed on 18 September 2012

Rheingold, H. (2000) *The virtual community: Homesteading on the electronic frontier*, MIT Press, Cambridge, revised edition

Rifkin, J. (2000) *The age of access: How the shift from ownership to access is transforming capitalism*, Penguin Books, London

Tamura, T. (2005) Japanese feeling for privacy. Proceedings of the 2nd Asia Pacific Computing and Philosophy Conference, Hongladarom, S. (ed.) Novotel Hotel, Bangkok, Thailand, January pp 88-93

Tavani, H. T. (2011) *Ethics and technology: controversies, questions, and strategies for ethical computing*, Hoboken, N. J., John Wiley, third edition

Tsai, C. Y., and Chiu, C. C. (2004) A purchase-based market segmentation methodology, *Expert Systems with Applications*, Vol. 27 pp 265-276

Valenzuela, S., Park, N. and Kee, K. F. (2009) Is there social capital in a social network site? Facebook use and college students' life satisfaction, trust, and participation, *Journal of Computer-Mediated Communication*, Vol. 14 pp 875-901

Wallace, P. (1999) *The psychology of the internet*, Cambridge University Press, Cambridge

Weckert, J. (2003) *On-line trust, The impact of the internet on our moral lives*, Cavalier, R. (ed.) Suny Press, Albany, NY pp 95-117

Weckert, J. and Adeney, D. (1997) *Computer and information ethics*, Westport, Connecticut/London, Greenwood Press

Wellman, B. and Gulia, M. (1999) Net-surfers don't ride alone: Virtual communities as communities, Wellman, B. (ed.) *Networks in the global village: Life in contemporary communities*, Westview, Colorado pp 331-366

Young, Y. (2009) Online social networking: An Australian perspective, *International Journal of Emerging Technologies and Society*, Vol. 7, No. 1 pp 39-57

Zamir, O., and Etzioni, O. (1999) Grouper: a dynamic clustering interface to Web search results, Computer Networks: *The International Journal of Computer and Telecommunications Networking*, Vol. 31 pp 1361 – 1374

Zhao, P. and Zhang, C. Q. (2011) A new clustering method and its application in social networks, *Pattern Recognition Letters*, Vol. 32 pp 2109 - 2118

## Note on the contributors

Yeslam Al-Saggaf is a Research Fellow at the Centre for Applied Philosophy and Public Ethics (CAPPE) and a Senior Lecturer in Information Technology at the School of Computing and Mathematics, Charles Sturt University. He holds a Bachelor's degree in Engineering (with honours) in Computer and Information Engineering, from Malaysia, and a Master's in Information Technology and a PhD from Charles Sturt University, Australia. His research interests lie in the areas of privacy in social media and ICT ethics. He has published in those areas in a number of international refereed journals as well as presenting at a number of international conferences. His current research project focuses on professionalism in the ICT workplace. Contact details: School of Computing and Mathematics, Boorooma Street, Wagga Wagga, NSW 2678, Australia. Email: yalsaggaf@csu.edu.au.

Md Zahidul Islam is a Research Fellow at the Center for Research in Complex Systems (CRiCS) and Lecturer in Computer Science at the School of Computing and Mathematics, Faculty of Business, Charles Sturt University. He has received his Bachelor's degree in Engineering from Rajshahi University of Engineering and Technology, Bangladesh, Graduate Diploma in information science from the University of New South Wales, Australia and PhD in Computer Science (thesis titled *Privacy preservation in data mining through noise addition*) from the University of Newcastle, Australia. His main research interests include privacy issues for online communities caused by data mining, privacy preserving data mining, application of data mining techniques, and various data mining algorithms including classification, clustering, missing value imputation, data cleansing and data pre-processing. Email: zislam@csu.edu.au. Web: http://csusap.csu.edu.au/~zislam/.