Privacy landscape in online social networks

Agrima Srivastava* and G. Geethakumari

Department of Computer Science and Information Systems,
BITS Pilani,Hyderbad Campus,
Hyderabad, India
Email: agrimasrivastava1@gmail.com
Email: geetha@hyderabad.bits-pilani.ac.in
*Corresponding author

Abstract: These days a large number of people are actively using online social networks (OSNs). OSN users can freely interact with their digital friends and build and maintain their online as well as their offline relationships. Intentionally or unintentionally users share a lot of their personal information on these networks which results in privacy threats and unwanted privacy breaches. One of the major reasons for this is the lack of privacy awareness among users and their inability to effectively make correct use of privacy settings. Privacy in an OSN can be viewed from different perspectives but we mainly focus on user privacy. We present an elaborative privacy landscape where we compare and contrast previous literature, review existing definitions covering taxonomy and privacy concerns in OSNs, discuss different perceptions of privacy amongst users and some privacy preserving approaches to guarantee maximum privacy.

Keywords: privacy; online social networks; OSNs; privacy taxonomy; privacy perceptions; privacy enhancing tools; privacy mechanisms; trust.

Reference to this paper should be made as follows: Srivastava, A. and Geethakumari, G. (2015) 'Privacy landscape in online social networks', *Int. J. Trust Management in Computing and Communications*, Vol. 3, No. 1, pp.19–39.

Biographical notes: Agrima Srivastava is a research scholar in the Department of Computer Science and Information Systems at Birla Institute of Technology and Science-Pilani, Hyderabad Campus. Her interest areas are data privacy, social network analysis, data mining, machine learning, misinformation detection, trust, privacy preserving data publishing and information security.

G. Geethakumari is an Assistant Professor in the Department of Computer Science and Information Systems at Birla Institute of Technology and Science-Pilani, Hyderabad Campus. Her PhD thesis was titled 'Grid Computing Security through Access Control Modelling'. She has many international publications to her credit. Her areas of research interests include: grid computing, information security, access control modelling, parallel computing, cloud computing and cloud security challenges. She is a member of IEEE as well as a member of IEEE Computer Society. She is also a professional member of ACM. She has been a member of the Technical Program Committees of various IEEE international conferences.

1 Introduction

Online social networks (OSNs) are one of the biggest advancements that have happened in the past decade. Barnes (1969) first introduced the concept of social networks and described them as connected graphs in which the nodes represent entities and the edges represent their interdependencies. These entities can be an individual, group or an organisation and the edges between them can be their interactions, relationships, values, etc. Over a period of time OSNs have evolved, provided a platform for sharing and have become an integral part of our lives. Some of the popular online social networking sites that are being used nowadays are Facebook, Twitter, MySpace, LinkedIn, etc. To be a part of OSN, users create their profiles which are an online representation of an individual and they make relationships with other online users. This connection or relationship can either be bidirectional as in Facebook or can be unidirectional like Twitter. OSNs can be connection-based and used for dating, business, enforcing real life relationships, socialising, instant messaging or can be content-based and used for content sharing, resource recommendation, advice sharing, hobbies, entertainments and news sharing, etc. (Beye et al., 2010).

Individuals using these sites have an online as well as an offline relationship with each other. Users do not share their private details to everyone with whom they are connected offline instead they selectively disclose only a part of their information to some of them. When this relationship is replicated online then the same distance should be mapped online as well. Users should maintain a proper online social distance with other users with whom they do not want to share everything. This gives rise to the concept of privacy in OSN. Privacy is about having control over what we share. Any unwanted disclosure of information can lead to privacy breach. If an individual's privacy is breached and is not respected then they feel defiled and violated (Trepte and Reinecke, 2011).

In addition to what a user shares online, it is also important to restrict the information transmission between user and the third party applications. To provide engaging experiences, online social networking sites provide applications that can utilise and enhance the users' profile. These applications can be the games they play, a tool to add additional contents to the profile, etc. (Besmer and Lipford, 2010). As there is no free lunch in data privacy (Kifer and Machanavajjhala, 2011) these applications take away the publicly available user profile data such as name, date of birth, gender, interests, likes, etc., and can even access the data of users' friends even if they are not directly using the application. Hence, an individual's privacy alone does not depend on them but also depends upon the people with whom they share their information which gives rise to the issue of linked privacy.

In OSNs data and identity are very closely linked. Information has a scope and this scope is defined by the people with whom this information is shared. Privacy of information is keeping it within its scope. Disclosure of information beyond its scope leads to a privacy breach (Beye et al., 2010). The third parties are external entities and can mine personal sensitive data and use it for various purposes like targeted advertising, uncovering interaction patterns in business, stalking, cyber bullying, malvertising, phishing, social spamming, scamming, click jacking, detecting of hidden and implicit groups, sensing users' sentiments, etc. More than half a billion users are using OSNs and have shared their details online because it is easier to share than to hide an information in an OSN (Krishnamurthy and Wills, 2009).

The social capital is measured by the ability of users to interact in OSN. It can decrease significantly if a lot of privacy policies are being imposed and as a result users will not exchange ideas with ease. There are two ends of information disclosure, privacy and publicity, whereas the middle path defines sociality. The path to sociality is taken at the expense of privacy. If in the network there is no flow of information it becomes a static and asocial network. To stay social users should be digitally literate which would help them to define the boundaries for their private information.

The rest of the paper is organised as follows. In Section 2, we summarise the related work in the area and bring out the requirements to have a fresh approach to evaluate work done in the area of privacy in OSNs. Section 3 discusses privacy in general and explains privacy definitions described and adopted by different researchers. Section 4 gives a broader view of OSN and its privacy concerns and throws light on how sharing of personal identifiable information (PII) can be a threat to individuals. A lot of surveys have been carried out to study and understand privacy perceptions of people therefore Section 5 explains some of the selected extensive surveys carried out in the field of privacy and OSNs. To comprehend the importance of privacy and utilise privacy settings provided by almost all of the social networking sites many researchers have come up with privacy enhancing and preserving mechanisms therefore Section 6 discusses such mechanisms in details that provides some of the other deeper and meaningful insights about privacy in the network. In Section 7, we conclude the study and discuss the scope of future work in the field.

2 Related work

Study of privacy is being carried out even before the internet existed. Privacy is an important area and has its implications in fields like the wireless networks, wireless sensor networks, social networks, healthcare networks, data bases, data publishing, data mining, etc. This section aims to present a summary of some of the existing studies that have been carried out in the field of privacy for various domains.

Beye et al. (2010) surveyed different types of OSNs and classified them on the basis of their purpose. They distinguished different types of data that are contained in OSNs and identified associated privacy risks in relation to users and service providers. They discussed privacy protecting technologies like anonymisation, decentralisation, privacy settings management, encryption, awareness and law and regulations. Their work talks about different privacy issues faced by the users and some of the existing solutions to prevent privacy breach. Wu et al. (2010) had surveyed the recent research developments on privacy preserving publishing of graphs and the social network data. They categorised anonymisation techniques into three main categories, i.e., k anonymity-based privacy preservation via the edge modification, probabilistic privacy preservation via edge randomisation and privacy preservation via generalisation.

Aggarwal and Yu (2008) provided a review of the state-of-art methods for privacy. Methods like randomisation, k anonymisation and distributed privacy preserving data mining are extensively discussed in the study. They had provided a review of major algorithms for each of the methods and variations for different techniques. They had given an overview of a number of diverse application domains for which privacy preserving data mining methods are useful. There is a lot of demand for exchange and

publication of data. Data in its actual form cannot be published because it contains sensitive information about individuals and hence a need for privacy preserving data publishing (PPDP) mechanism came into existence. In PPDP data is transformed before it is being released so that the individual's actual attributes cannot be inferred. In a study Fung et al. (2010) have summarised and evaluated different approaches for PPDP.

Kumarguru and Cranor (2005) have described the methodology, questions and results obtained used by Westin to create a privacy index. Westin has conducted over 30 surveys and created privacy indexes for each of them to summarise the results and to show the concerns of privacy. He classified the public into three categories namely

1 the high or the fundamentalist

2 the medium or the pragmatics

3 the low or the unconcerned.

Many privacy researchers have used their privacy indexes as a benchmark and have used their own surveys to classify people. Li (2010) review different approaches proposed to tackle the privacy issue in online social networking sites. They categorised the current approaches into three categories which are approaches addressing end users' participation, security automation-based on machine learning algorithms and privacy preserving by issuing a decentralised architecture for social networking services.

Toch et al. (2012) analysed the privacy risks associated with several current and prominent personalisation trends, namely social-based personalisation, behavioural profiling and location-based personalisation. They survey user attitudes towards privacy and the technologies that can reduce the privacy risks like the pseudonymous personalisation, client side personalisation, distribution, privacy-preserving techniques, user controls and feedback and privacy-preserving location tracking. Shen and Pearson (2011) showed that the privacy enhancing technologies (PETs) can help to address different types of privacy harm to employees, customers and the data subjects. They have discussed PETs for anonymisation, for network invasion protection, identity management where they discussed about the credential and trust management, data processing, privacy preserving data mining, management of privacy in data repository and policy checking PETs, etc. They have also given an overview of the current PETs, their enhancements and the Solove's taxonomy which we will be discussing in next section.

In Table 1, we show a comparative evaluation of the related literature. We have categorised the related work into five broad categories namely

1 definition and general study

2 data publishing techniques

3 tools

4 statistics and results

5 user privacy.

A √ symbol indicates that the research work contributed to particular category and an X symbol signifies that research work did not deal with that specific category. In comparison with the above literature our work discusses definition, general study, various tools, statistics and the future directions for preserving privacy. We give a holistic view of technologies and mechanisms used for understanding and strengthening privacy.

Understanding privacy is not an easy task as its meaning differs greatly from one context to another and hence we summarise the concept of privacy given by some of the elite researchers around the globe. To understand how well do people know about the importance of privacy we analysed different studies carried out in this area and compiled aim, methodology, results of their study and drew meaningful conclusions from the same. In this work, we cover some of the important privacy mechanisms used in the field and also explain them in detail in the subsequent sections. In the next section, we will discuss the privacy taxonomy and throw light on the meaning and definition of different facets of privacy.

Table 1 A comparison of related surveys carried out in the field of privacy in OSNs

Author	*Definition and general study*	*Data publishing techniques*	*Tools*	*Statistics and results*	*User privacy*
Beye et al.	√	X	X	X	√
Wu et al.	√	√	X	X	X
Aggarwal et al.	√	√	X	X	X
Fung et al.	√	√	X	X	X
Kumarguru et al.	√	X	X	√	√
Li et al.	√	X	√	X	√
Toch et al.	√	X	√	X	√
Shen et al.	√	X	√	X	√

3 Understanding taxonomy of privacy

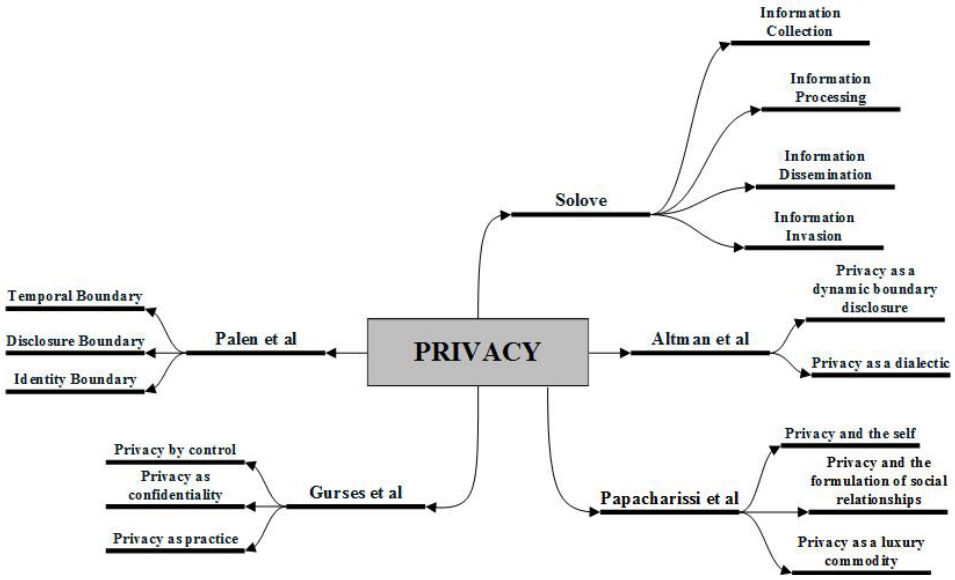
Privacy is derived from the word privatus meaning separated from rest. Privacy does not have a specific definition as its degree differs from an individual to individual. It greatly depends on culture and nation. In a broad sense privacy can be described as selective revelation about self. According to Warren and Brandeis (1890), privacy is "the right to be let alone". Westin and Blom-Cooper's (1970) definition says that privacy "is the claim of individuals, groups or institutions to determine that how, when and up to what extent is the information about them are communicated to others".

Figure 1 shows a privacy taxonomy where we have considered privacy definitions by Altman and Taylor (1973), Altman (1975), Palen and Dourish (2003), Solove (2006), Diaz and Gürses (2012) and Papacharissi and Gibson (2011). The details of their classification are described as follows.

Altman privacy theory (Altman and Taylor, 1973) views privacy management as a dialectic and dynamic boundary disclosure.

- Privacy as a dialectic: If privacy is considered as a dialectic then it greatly depends upon expectations and experience of users and the ones with whom they interact.
- Privacy as a dynamic boundary disclosure: Privacy as a dynamic boundary regulation process is a continuous process of negotiation to decide a boundary between public and private.

Figure 1 The privacy definition taxonomy



According to Palen and Dourish (2003), at any given time there has to be a proper balance between privacy and publicity, self and others and past and future. On the basis of this they have described three boundaries as the centre for characterisation of privacy management which are explained as follows:

- Disclosure boundary: Being a part of a society people share information which comes at the cost of privacy. The individual should decide about an item's visibility. There has to be a proper boundary to decide the same and this is the disclosure boundary.
- Identity boundary: This is a boundary between self and the other.
- Temporal boundary: This is a boundary between past and future. According to observations the critical instances of information disclosures are related to each other. An event in the past affects the present.

According to Diaz and Gürses (2012), classification privacy problems can be divided into three categories which are

1 privacy as control

2 privacy as confidentiality

3 privacy as practice

- Privacy as control: The organisations offering electronic services are responsible to collect PII and process it. If this information is disclosed to other party or a broader public then it leads to a privacy violation. Privacy is articulated through policies which is defined by users (privacy settings) or organisations (access control).

  For, e.g.: Privacy settings, access control, auditing, purpose-based access control are some of the examples of privacy research in this paradigm.

- Privacy as confidentiality: This mainly focuses on the data disclosure problem. The privacy is breached if particular information goes beyond its visibility scope. Privacy as confidentiality is to enable a minimal disclosure such that the information cannot be linked back to an individual.

  For, e.g.: Anonymous authentication protocols, anonymous communication networks and private retrieval.

- Privacy as practice: Privacy is not just a matter of individual it is indeed a matter of social concern. Users often decide their privacy and its dimensions based on the community they live in. This mainly is concerned with the feedback and creating general awareness amongst the individuals as well as the data collectors. The main privacy concern is that it becomes difficult for the user to understand how they should control their data and if this information is disclosed what inferences could be made on it.

  For, e.g.: P3P and privacy mirror are the technologies adapting to privacy as a practice.

Autonomy is the ability to build our own path without any external influence or impediment. Based on autonomy Papacharissi and Gibson (2011) view privacy as self, privacy as formulation of social relationship and privacy as luxury commodity.

- Privacy and the self: The identity of an individual is unique but fundamentally social. The sense of self of an individual is developed through collaborative and collective experiences of the individual's social interactions. The performance of the self should sense to multiple audiences and public without compromising our sense of who we truly are.

- Privacy and the formulation of social relationships: Privacy enables the existence of relationship and community. If we share every information about us to the public then the information loses its meaning and inherent value. The individuals have online social relationships with the other individuals and hence they share their information with them. Having social relationships encourages loss of privacy and hence is a challenging task to prevent on such platforms.

- Privacy as a luxury commodity: The web accessible platforms offer services of social nature. They take the personal information and make money out of it. Information is treated as a commodity and thus makes the information privacy a luxury commodity.

The most comprehensive privacy taxonomy so far is the *Soloves's taxonomy* (Soloves, 2006) which characterises the four main stages of information. The privacy problems related to each of them which are stated as follows:

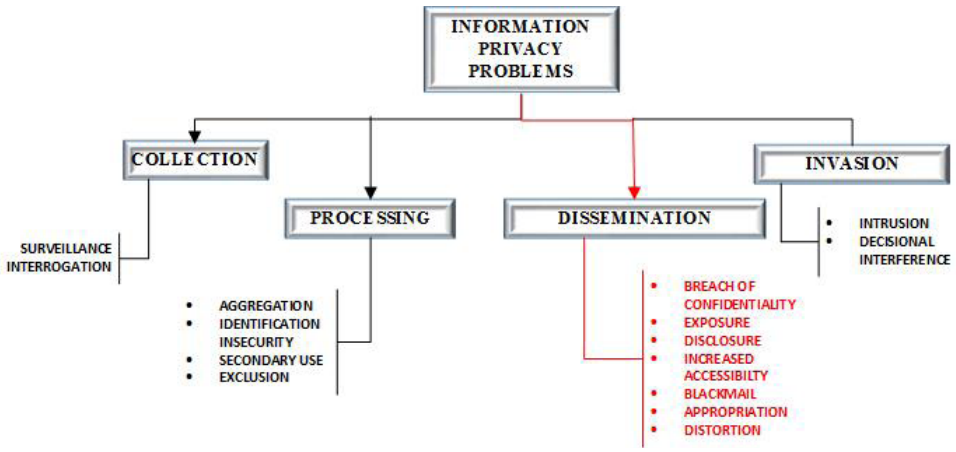
- Information collection: This stage deals with the process of data collection and privacy violation. Surveillance and interrogation are viewed as problematic in this stage.

- Information processing: This stage deals with the usage, storage and manipulation of collected data. Aggregation, identification, insecurity, secondary use, exclusion are the harms associated with the stage.

- Information dissemination: This stage deals with the revelation of personal data or the threat of spreading information. Breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, distortion is the major privacy concerns with information dissemination.
- Information invasion: This stage deals with privacy problems when there are attacks on established systems. Intrusion and decisional interference are the privacy problems for the stage.

In this paper, we will be following the Solove's taxonomy and will mainly concentrate on the information dissemination part. Figure 2 gives the diagrammatic representation of the Solove's taxonomy. We will be discussing the problems such as breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation and distortion, etc. The definition of privacy is not limited to the above classification and differs from context to context. Privacy is a serious concern and hence every individual should understand its importance and protect their privacy. Sharing of information on a platform provided by OSNs has become a common practice. If this information is used in a way which is not desired by the user their privacy gets affected. In the next section, we will be discussing about the privacy issues of sharing the PII online and the effects of identity, link and attribute disclosure.

Figure 2 The Solove's taxonomy (see online version for colours)



4 Privacy concerns of OSNs

OSN is a web-based service that allows individuals to construct their digital profiles within a bounded system. Using such networks users can interact with each other and build and maintain relationships (Ellison, 2007). Data security is one of the biggest challenges in OSN. Where data security is important data privacy is no less. Privacy is multi-faceted, at one instance the individual would want some information to be disclosed to everyone whereas at the other instance he may not like sharing it to the entire friend list (Gross and Acquisti, 2005). A wealth of personal information is shared online on a daily basis by individuals. Sharing their information makes them active and popular

on these networking sites but if they do not properly control their PII it can be misused leading to privacy violation.

Figure 3 The effects of disclosure (see online version for colours)

4.1 Categories and effect of disclosures

The pervasive use of OSN gave rise to huge privacy concerns (Gundecha and Liu, 2012). PII is one of the most important concepts of information privacy which is collected during an electronic service. OSN is enriched with data like the photos, videos, likes, interests, address, date of birth, gender, education, work, etc., and any unwanted disclosure of these attributes can harm the privacy of individuals (Acquisti and Gross, 2009). Identity disclosure, link disclosure and attribute disclosure are the three main categories of disclosure and are explained as follows:

- Identity disclosure: Identity disclosure results in the disclosure of the identity associated with the entity. For, e.g., if a particular person is a member of any political or religious group and does not want his presence to be known by others, identity disclosure could do a serious harm to the person.
- Link disclosure: Link disclosure results in the disclosure of sensitive connection or relationship that a particular entity has with the other actors.
- Attribute disclosure: Attribute disclosure is the disclosure of the sensitive attributes of an entity. For, e.g., sensitive contents like the text message, the timestamp, the frequency of interaction, etc. (Liu et al., 2008).

Figure 3 gives an overview of some of these attributes and its ill effects on their disclosure. For, e.g., photos and videos can be morphed and the users can be threatened, blackmailed and defamed. Likes and interests of individuals reveal a lot about them and can lead to formation of controversial opinion about them. Using address the schedule of the person can be known and this can result into a criminal attack or burglary. Combining address, date of birth and gender of an individual their Social Security number (SSN)

number can be determined resulting in ID theft or impersonalisation. E-mails and phone numbers can be misused for targeted advertising which leads to unnecessary interruptions and spam. These were some of the problems associated with the disclosure. To prevent it users should know and understand the meaning of privacy. Studies were carried out to understand the online sharing behaviour of people and to know how well do people care about their privacy and the way to implement privacy in their offline and online environment. In the next section, we will discuss some of those studies, their methodologies and the results obtained.

5 Privacy perceptions of users in OSNs

In this section, we aim to give insights on different studies that were carried out by researchers and understand some of the aspects of privacy like

a relevance of privacy

b OSN privacy threats

c reason for sharing personal information, etc.

Some of those important works are discussed as follows:

Liu et al. (2011) have measured disparity between actual and the desired privacy settings of objects shared by the users. Their analysis was centred on knowing the ideal privacy settings and the actual privacy settings of the users. The survey carried out by them selects ten photos for query and collects ideal and actual privacy settings for the same. This analysis revealed that the users are uploading significant amount of content on Facebook and almost half of the content is shared with the default privacy settings which is desired by just 20% of the users. This study suggested that the default privacy settings are poorly chosen by the users and in most of the cases their expectations did not match the reality. Their work provides a deep statistical insight on the differences between user expectations and reality but does not mention the tools which would help users bridge this gap.

Stutzman and Kramer-Duffield (2010) have looked at the association between network compositions, expectancy violation and interpersonal privacy practices of having a *friends only* profile. They drew Petronio's (2002) theory of communications privacy management (CPM) which discusses iterative process of rule development. It regulates *who* to tell *what* and boundary coordination which develops disclosure ownerships and permeability rules in the network. Boundary turbulence refers to the dynamic process of maintaining and negotiating boundaries to maintain personal disclosures. They identified a range of factors like gender, network size, weak tie expectancy violations and increasing level of interpersonal practices with privacy behaviour in the social network site 'Facebook'. Their work concludes that the act of having a *friends only* profile is discretely notable. One of the limitations of their work is that the data is self-reported and has limited accuracy and recall. Their study also has the potential for non-response bias as under representative of males and non-white individuals were considered.

Wang et al. (2011) have investigated regrets associated with the posts of users. They targeted sensitive topics, contents with strong sentiments, lies and secrets. They conducted a survey and concluded that the participants regretted posting illegal drugs and alcohol use, posting photos depicting a different image of themselves, posting religious

and political belief that caused debates. All these practices offended people and damaged relationships. The main reason why people post sensitive content online is either out of depression, frustration or anger. Comments made out of profanity, personal and family issues, expressing work and company in a negative way, etc., are too sensitive to be made online. Some of them do not use privacy settings appropriately and posts sensitive things out of ignorance. However, this work was an in depth study but the solutions for the same were not proposed.

Johnson et al. (2012) recruited 260 Facebook users to install a Facebook application that surveyed the users' privacy concerns, their network compositions, the sensitivity of the posted content and their privacy preserving strategies. Their study showed that 86.2% of participants were unconcerned with the threats of strangers viewing their profile content. They could figure out that the threats from inside the network were more of a concern to the users. Their method inherently introduces bias as at least two people refused to participate. The sample used in their work was biased toward users who are unconcerned with privacy.

Sleeper et al. (2013) have looked at the types of contents that the users were sharing currently. Questions like why they choose not to share different types of content, how much will they share if they know the intended audience and what attributes define the groups with whom the users want to share their content were looked into. The study revealed that participants are self-centred because they wanted to manage the way they presented themselves to various audiences. The participants indicated that they would have shared about half of the self-censored content if they would have the ability to optimally target audience. One of the biggest demerits of their study was the small sample size and therefore the results were difficult to generalise. The method employed to collect the data was the diary study which made the data biased.

Asking a user to directly evaluate the privacy concern is related to the emotional response and the results obtained are often biased. Braunstein et al. (2011) have proposed an indirect technique for measuring content privacy concerns. A total of three surveys were carried out, the first one being an initial survey that does not mention about privacy or security, the second one to emphasise the security and privacy risks and the third one to explicitly focus on privacy. The privacy ratings were sensitive thus the privacy rankings were used as a ground truth for measuring. Model-based and score-based ranking were the two ranking methods employed in the study. Using the model-based ranking the likelihood of content retrieval in each of these studies was compared with the results of the direct study. Using the scoring function the questions were clustered into groups and the correlation was used to calculate the association between them. They have suggested mechanisms for translating responses to indirect questions into privacy ratings and proved that this mapping highly preserves relative rankings of content types from direct privacy surveys as more privacy language is introduced. In this study, the use of privacy language is made extensively and hence according to the hypothesis the respondents might have adjusted their response to accommodate the goals of the experiment thus making the data biased.

In Table 2, we show the merits and the demerits of different privacy perceptions of users in an OSN. The study reveals that mostly it is the unawareness of privacy and its importance that results in a privacy breach. People find managing privacy settings a time consuming and confusing task. Therefore, there is a dire need for some efficient tools and mechanisms to ensure privacy. Many researchers have come up with privacy preserving

tools and efficient mechanisms to resolve the problems stated above. In the next section, we will be studying the different mechanisms by which privacy can be enhanced and preserved.

Table 2 A comparison showing the pros and cons of different privacy studies in the field of OSNs

Author	*Pros of the study*	*Cons of the study*
Liu et al.	Measured the disparity between actual and the desired privacy settings	No mention of tool/method is made
Stutzman and Kramer-Duffield	Studied association between network composition, expectancy violation and interpersonal privacy practices of having friends only profile	Self-reported data, limited accuracy and recall, non-response bias
Wang et al.	Investigated the regrets associated with users' posts	No solutions were provided
Johnson et al.	Study of users' privacy concerns, their network compositions, sensitivity of the posted content privacy preserving strategies	Sample used was biased toward users who are unconcerned with privacy
Sleeper et al.	Studied the sharing behaviour	Small sample size, difficult to generalise, diary study resulted in biased data
Braunstein et al	Indirect technique for measuring content privacy concerns	Use of privacy language is made extensively, respondents might have adjusted their response thus making the data biased

6 Mechanisms for preserving privacy

In this section, we will be reviewing the tools used for preserving and enhancing privacy. We would also discuss some existing privacy mechanisms built on structural analysis and psychometrics. Some of the important works in each of these areas are discussed as follows:

6.1 Tools for preserving and enhancing privacy

Fang and LeFevre (2010) have proposed 'PrivacyWizard' which is a tool to automatically configure the privacy settings of a user's profile. The fact that the real users conceive their privacy preference according to an implicit set of rules is used to build the model of privacy wizard. The users were asked to assign the privacy label, i.e., (allow, deny) for a profile item with respect to the friend. If for a friend f and profile item i the preference, i.e., pref (i, f) = allow, then that means that the friend f is allowed to see the profile item i. To intelligently request the user to provide labels to the most informative friends the wizard uses the uncertainty sampling as a particular active learning technique and then the classifier labels the rest of the friends automatically. The wizard involves low effort, gives high accuracy, supports graceful degradation and works on limited data. The major

limitation of this research is that the wizard was tested on a small data size of 45 Facebook users and does not look into the inference and shared data ownership issues.

Ghazinour et al. (2013) have presented a tool 'YourPrivacyProtector' for recommending privacy settings to users. Users' personal profile, interests and their privacy settings on their photo albums were collected which were used to construct the personal profile of a user to find the similarities between the individuals. According to Westin, people can be put into three groups namely *fundamentalists*, *pragmatics* and *unconcerned*. The tool uses decision tree to infer the profile types of each user and k nearest neighbour classifier for determining the privacy settings of the class the user belongs to. The results could have been tested on a larger dataset to demonstrate the scalability of the model. The tool does not consider the sensitivity of the data items being shared which would otherwise have given better and improved results. If the user takes photos of nature, actor, buildings, etc., and wants everyone to view their album and sets it visible to public then this does not imply their unconcerned nature. Such cases are not identified and dealt separately in the study.

Mazzia et al. (2012) have introduced PViz which is an interface that corresponds to the way the OSN users model groups and privacy policies. The main goal of the tool is to make the users understand the visibility in a natural way. They extracted a hierarchy of communities according to a simple recursive process where the network is partitioned into communities and each of the community is treated as another network which is partitioned again. This is continued until no further partitioning can be done that could improve the modularity. PViz generates the initial set of labels for the communities and help the users to visualise and understand their privacy policies. Their study and results show that PViz performs better than many of the tools in the present state of art. The evaluation was carried out on 20 participants which is quite less a number to generalise the efficiency and accuracy with which the tool performs and hence adds to the demerit of the study.

Bickzok and Chia (2013) have defined online privacy interdependence and have modelled its impact through an interprivacy game. A could easily embarrass B by sharing B's photos or videos or by tagging B in an appropriate video. They modelled the game for one application and two player case with the following details:

- Assumption:
  1 players are non-cooperative
  2 all players have a 'friend' connection
  3 only applications that ask for privacy of friends are considered.
- Players: The interprivacy game has two players.
- Strategies: The decision made here is to whether install (i) or not install (n) an application, i.e., $S = i, n$.
- Payoff: Both the positive and the negative externalities could emerge from the decisions of two players, here the positive externality means having more users installed the applications and the negative externality could be the privacy concerns for an application installed.

The externalities caused by privacy interdependence and their effect on the user and the vendor welfare equilibrium were analysed. This study does not take into consideration the amount and sensitivity of personal data stored in the given OSN user account which might provide more realistic results.

Kafali et al. (2012) have developed PROTOSS which is a run time tool for detecting the privacy leakages in OSNs. The main technique involved here is model checking. PROTOSS uses network and agreement information to decide whether agreements are met or not. The two of the important techniques used in their approach are extracting of commitments and checking models for the system. Commitment is an agreement from a debtor to a creditor about a property for a specific condition which can be represented as C (debtor, creditor, condition, and proposition). To verify that a given property holds or not the model checking algorithm is used. System is viewed as a state transition graph and the property as logic formula. A model checking algorithm checks that whether the system model satisfies the property or not. The drawback of the study is that it does not talk about the scalability of the tool.

These were some of the tools and strategies that were developed and used for preserving and enhancing privacy in OSNs. The degree of security and privacy also depends upon graph theoretical properties of the social graph. In the next subsection, we will discuss some of those mechanisms where the structure of the graph is used to give fundamental insights on the degree of privacy.

6.2 Privacy using structural analysis

Privacy degree in an OSN strongly depends upon the topological properties of social graph. In this subsection we give an overview of such studies where a relation between the structure of a graph and privacy is drawn. A social network can be represented using an undirected graph $G = (V_G, E_G)$, with vertices $V_G = (v_1, \ldots v_n)$ and $E_G = (v_i, v_j)$ where $v_i, v_j \in V_G$ and $i \neq j$. Here, the nodes are social actors and the edges are the relationships between the actors.

According to Cutillo et al. (2011), the achievable security and privacy also depend upon the graph theoretical properties of the social graph. They analysed the relationship between the social network topology and the achievable privacy. The three main metrics that they looked into were the *node degree*, *clustering coefficient* and *mixing time*. The effect of each of them is explained as follows:

- Node degree: If the social graph is denoted by $G(V, E)$ where $\deg(v)$ is the degree of the vertex v; p_{mal} is the probability that a new friend n of v is a malicious user then the event of befriending the friends $F_{mal}(v)$ of v follows a binomial distribution. If user n gets access to the sensitive data of v then the disclosure can turn out to be a severe damage and hence the out degree of a node is directly proportional with its usage control.
- Clustering coefficient: The clustering coefficient $c(v)$ is defined as the number of existing links between the nodes $e_{deg(v)}$ divided by the total number of possible links which is equal to $\frac{\deg(v)\deg(v)-1}{2}$. The tighter the friend set the broader is the disclosure of sensitive data to the user's contact.

- Mixing time: For a random walk the number of hops to reach a steady state distribution is called the mixing time. A small mixing time is required to enhance the security and privacy performance.

However, the study does not validate the results obtained after comparing the metrics and the reason for selecting only the above mentioned metrics is not specified clearly in the study.

Yildiz and Kruegel (2012) have proposed a solution to control the privacy by automatically detecting social cliques among the friends of the user. This social clique identified is used to create a friend list for the user. Their proposed algorithm starts by an initial clique C that consists of the number of participants P. The participants are the people who are directly related with the data item shared. In each iteration, the clique is expanded by adding the candidates to it. Addition of the candidate maximises the heuristic function f. The algorithm stops when the addition of the candidate does not satisfy the function. Out of all the candidates the candidate that has the highest heuristic value is considered. Several clique expansion techniques like the CLQ, $BAND_k$, IN_k were used. They proposed that the $BAND_2$ and IN_3 schemes were accurate to form the final exposure set having the list of people who could view a particular shared data item.

Often in a group of friends if a personal secret of friend A is known by a friend B then after some time almost the entire group knows about it. Using social networks the structure and the evolution of social systems becomes easy to understand. Lind et al. (2007) have studied the general model of information spread which is suited for different kinds of social information. They proposed measures like spreading factor and spreading time which are accessible neighbourhood around the node and the minimum time to reach such neighbourhood respectively. These properties give an insight about the private information spreading in the network. However, factors like decreasing the spreading factor and increasing the spreading time which would be needed to prevent gossip and spread of private information was not discussed.

Passing a private information from node A to the node B about the node C (who is not present at the scene) is known as gossiping and can affect the relationship between A-B, A-C and B-C. Unlike a rumour which is usually some issue or matter related to public concern, a gossip deals with the behaviour and life of an individual. Any analysis of spreading private information is done at the triad level or at a higher level. Shaw et al. (2011) have revealed that how the information that they had passed along one edge can affect the strength of the other edges. They conducted experiments and concluded that gossip will decrease the network clustering and the average node degree. In this work, the assumptions made are highly simplistic. The study considers only the negative aspect of gossip whereas gossip could be positive and conducive which is not justified.

As described earlier a lot of research exists for privacy concerns in OSN data that is owned by various organisations and how can that data be shared without revealing the identity of an individual. But not much attention has been paid for the privacy risk of the users that comes by information that has been explicitly shared by them on their profiles. Privacy is abstract; something that exists but when it comes to measuring the privacy it becomes a challenging task. In the next subsection, we discuss the relation between privacy and psychometrics and discuss some of the works carried out in the area for measuring privacy.

6.3 Privacy and psychometrics

Psychometrics is a field of study that is concerned with psychological measurement. Unlike height and weight privacy does not have an exact measuring scale. Its value depends upon a lot of other hidden traits. Many users in an OSN share their digital personal space. Identity theft, stalking, target advertising, online victimisation, etc., are some of the privacy risks involved with openly sharing PII on the network. Though indirectly but using psychometrics the privacy leaks can be measured. Some of the works in the similar lines are explained as follows:

In Liu and Terzi (2009), the authors have shown a way to measure privacy using two parameters namely

1 sensitivity

2 visibility.

Sensitivity and visibility of information depends on the willingness of the people for sharing particular information. Sensitivity of an attribute is directly associated with the privacy risks. An item that is highly sensitive means that it is not frequently shared by the people and vice versa. Visibility on the other hand is a measure of information spread. To measures privacy the following formula was used,

$$PR(i, j) = \beta_i * V(i, j) \tag{1}$$

where $PR(i, j)$ is the privacy score for a profile item i for user j. β_i is the sensitivity of the profile item i and $V(i, j)$ is the visibility of the profile item i for a user j. To calculate the overall privacy score of the user j the following formula is used

$$PR(j) = \sum_i PR(i, j) = \sum_i \beta_i * V(i, j) \tag{2}$$

where $PR(j)$ is the overall privacy score for user j which is the summation of all the attributes i for a user j.

Here $V(i, j)$ using the item response theory (IRT) is calculated as:

$$PR\left(R(i, j) = 1\right) = \frac{1}{1 + e^{\alpha_i(\theta_i - \beta_i)}} \tag{3}$$

where α_i is the item's discrimination, θ_j is the attitude of user j, i.e., being an extrovert or an introvert, β_i is the profile item's sensitivity. They have used IRT model for all the computations and all the parameters are estimated using the maximum likelihood and expected maximisation. This mathematical model can fit well to the observed data and the privacy scores calculated using IRT model has an intuitive interpretation. In order to calculate the privacy scores the use of latent trait theory gives realistic and practical results. Though there are different IRT models (Rasch model, the two parameter logistic model, three parameter logistic model, etc.) available, the reason to select the two parameter model is not mentioned in the study.

Guo and Chen (2012) have introduced utility aspect into privacy settings and allowed users to maintain a proper tradeoff between privacy and utility by developing a method that could derive implicit utility preference from privacy settings. They have used IRT model to find the probabilistic relationship between the users' ability and their answers. The two parameter logistic model as stated in equation (3) was used for the calculations.

If two people are sharing the same number of different items then this does not necessarily mean that their privacy concerns will be the same. Here, the IRT model provides solutions and caters to such kind of problems as well.

Using the latent trait modelling they proposed a utility item model. For every user in the training set, a pair of (θ, ϕ) was derived where θ denotes the privacy concern and ϕ denotes the utility rating which corresponds to (p, u) where p and u were privacy and utility ratings respectively. The proposed algorithm aims at maximising the utility while keeping the privacy concern intact but does not look into setting the item weights for a users' utility preference which is an important issue. Measuring and ensuring privacy of an individual is a challenging task and psychometrics provides solutions to most of the privacy measuring problems. These were some of the existing works on the area of privacy. In Table 3, we show the merits and the demerits of different privacy mechanisms for achieving privacy in an OSN.

Table 3 A comparison of different mechanisms for achieving privacy in OSNs

Author	*Pros of the study*	*Cons of the study*
Fang and LeFevre	App automatically configures privacy settings low effort, high accuracy graceful degradation works on limited data	Tested on small data inference issues were not looked into
Ghazinour et al.	Privacy settings recommender system	Small dataset used, sensitivity of dataset is not taken care of
Mazzia et al.	Performs better than many other tools	Small dataset used
Biczók and Chia	Privacy interdependence was studied	Sensitivity of data stored in an OSN account is not taken care of
Kafali et al.	Detects privacy leakages in an OSN	No mention of, scalability of the tool is made
Cutillo et al.	Established relation between privacy and graph theoretical property	Results are not validated
Yildiz and Kruegel	Controlling privacy by detecting social cliques	Sensitivity of the data item being shared was not considered
Lind et al.	Studied information spread and factors affecting it	Factors that would decrease the spreading factor was not mentioned
Shaw et al.	Studied the effect of information spread of one edge on other	Positive effect of gossip is not considered
Liu et al.	Used IRT for measuring privacy	Model selection is not justified
Guo and Chen	Ensures utility-based privacy	Does not looks into setting the item weights for a user's utility

7 Conclusions and future directions

We presented a detailed study of user privacy in OSNs. We proposed the privacy taxonomy covering and explaining most of the privacy definitions provided by the researchers around the globe. This study also discusses some of the tools that have been proposed and built to meet and enhance privacy requirements of the user. We also bring

out different privacy perceptions of users on issues like privacy and its importance, OSN privacy threats and the reason for sharing personal information. Our study examines the privacy mechanisms through the prism of network structure and quantification of privacy leaks to ensure maximum privacy protection in an OSN.

Though a lot of work has been proposed in this area still this field has many interesting future research directions. Some of them are listed and explained as follows:

- Privacy is abstract and hence measuring privacy is a challenging task. Researchers have used a concept called the privacy score/privacy quotient. It is a score given to the user on the basis of the items being shared in an OSN using which privacy of the user can be measured effectively (Liu and Terzi, 2009; Srivastava and Geethakumari, 2013). Some of the tools discussed earlier ensure privacy but does not emphasise on measuring the sensitivity of the data being shared. Measuring the sensitivity of various data items in the profile would increase the accuracy and would provide more practical results. This study is in the nascent stage and a lot can be explored on the similar lines.
- Trust is a belief that an entity will behave in an expected manner. Privacy and trust go hand in hand and quantifying direct and indirect trust will help preserve the privacy of an individual effectively. Offline people do not share their information to anyone and everyone. They selectively disclose their private information. The same behaviour is difficult to replicate online. To minimise the unwanted information disclosure in an OSN a coarse grained privacy mechanism where the information can be shared to 'close friends' to prevent privacy leaks is being followed extensively. This however does not guarantee an effective privacy preserving mechanism. Incorporating trust before sharing private information in the network would ensure a better privacy protection. This area has many unanswered questions and a lot of future scope.
- Data in its original form usually contains sensitive information about individua0ls, and if that data is published as it is will lead to privacy violation. Currently, there are many practices and policies indicating the types of data that has to be shared or can be published. This practice however is not enough to preserve privacy and can result in an unwanted disclosure. PPDP (PPDP) provides ways for publishing useful information and also preserving data privacy. Many researchers have already come up with different proposals on PPDP. Some of the well-known ones are *k anonymity*, *l diversity*, *t closeness*, *differential privacy*, etc. One of the biggest challenges in this area is to reduce the possibility of inference attacks using which the identity of an individual can still be compromised.
- Most of the social networking sites are linked with third party applications and many unconcerned users unknowingly exchange their private data in return for the consumer benefits that they receive online. These applications have an access to the users' data as well as the data of its neighbours in the network even if the neighbours/friends are not using the application. Avoiding such unwanted linked data privacy leaks is one such challenge in the field and a lot can still be explored in this area contributing to the field of privacy preserving social network data publishing.

A single inference that can be drawn out of the work is that it presents entire user privacy landscape covering various aspects like the privacy taxonomy, privacy concerns of OSN users, different user privacy perceptions and many privacy preserving mechanisms. This work would provide a background for budding privacy researchers to explore and solve many unaddressed user privacy challenges in the field of OSN.

References

Acquisti, A. and Gross, R. (2009) 'Predicting Social Security numbers from public data', *Proceedings of the National Academy of Sciences*, Vol. 106, No. 27, pp.10975–10980.

Aggarwal, C.C. and Yu, P.S. (2008) 'Privacy-preserving data mining: models and algorithms', *Advances in Database Systems*, Vol. 34, Springer.

Altman, I. (1975) *The Environment and Social Behavior: Privacy, Personal Space, Territory and Crowding*, Brooks/Cole Pub. Co., Inc., Monterey, CA.

Altman, I. and Taylor, D.A. (1973) *Social Penetration: The Development of Interpersonal Relationships*, Rinehart & Winston, Holt.

Barnes, J.A. (1969) 'Graph theory and social networks: a technical comment on connectedness and connectivity', *Sociology*, Vol. 3, No. 2, pp.215–232.

Besmer, A. and Lipford, H.R. (2010) 'Users'(mis) conceptions of social applications', *Proceedings of Graphics Interface 2010*, pp.63–70, Canadian Information Processing Society.

Beye, M., Jeckmans, A., Erkin, Z., Hartel, P., Lagendijk, R. and Tang, Q. (2010) *Literature Overview-Privacy in Online Social Networks*.

Biczók, G. and Chia, P.H. (2013) 'Interdependent privacy: let me share your data', in *Financial Cryptography and Data Security*, pp.338–353, Springer.

Braunstein, A., Granka, L. and Staddon, J. (2011) 'Indirect content privacy surveys: measuring privacy without asking about it', *Proceedings of the Seventh Symposium on Usable Privacy and Security*, p.15, ACM.

Cutillo, L.A., Molva, R. and Onen, M. (2011) 'Analysis of privacy in online social networks from the graph theory perspective', *Global Telecommunications Conference (GLOBECOM 2011)*, pp.1–5, IEEE.

Diaz, C. and Gurses, S. (2012) 'Understanding the landscape of privacy technologies', *Proc. of the Information Security Summit*, pp.58–63, Prague, Czech Republic, May.

Ellison, N.B. (2007) 'Social network sites: definition, history, and scholarship', *Journal of Computer-Mediated Communication*, Vol. 13, No. 1, pp.210–230.

Fang, L. and LeFevre, K. (2010) 'Privacy wizards for social networking sites', *Proceedings of the 19th International Conference on World Wide Web*, pp.351–360, ACM.

Fung, B., Wang, K., Chen, R. and Yu, P.S. (2010) 'Privacy-preserving data publishing: a survey of recent developments', *ACM Computing Surveys (CSUR)*, Vol. 42, No. 4, p.14.

Ghazinour, K., Matwin, S. and Sokolova, M. (2013) 'Your privacy protector: a recommender system for privacy settings in social networks', *International Journal of Security*, Vol. 2, p.4.

Gross, R. and Acquisti, A. (2005) 'Information revelation and privacy in online social networks', *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, pp.71–80, ACM.

Gundecha, P. and Liu, H. (2012) 'Mining social media: a brief introduction', *Tutorials in Operations Research*, Vol. 1, No. 4.

Guo, S. and Chen, K. (2012) 'Mining privacy settings to find optimal privacy-utility tradeoffs for social network services', *Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Conference on Social Computing (SocialCom)*, pp.656–665, IEEE.

Johnson, M., Egelman, S. and Bellovin, S.M. (2012) 'Facebook and privacy: it's complicated', *Proceedings of the Eighth Symposium on Usable Privacy and Security*, p.9, ACM.

Kafali, O., Gunay, A. and Yolum, P. (2012) 'Protoss: a run time tool for detecting privacy violations in online social networks', *Advances in Social Networks Analysis and Mining (ASONAM), 2012 IEEE/ACM International Conference on*, pp.429–433, IEEE.

Kifer, D. and Machanavajjhala, A. (2011) 'No free lunch in data privacy', *Proceedings of the 2011 ACM SIGMOD International Conference on Management of Data*, pp.193–204, ACM.

Krishnamurthy, B. and Wills, C.E. (2009) 'On the leakage of personally identifiable information via online social networks', *Proceedings of the 2nd ACM workshop on Online Social Networks*, pp.7–12, ACM.

Kumaraguru, P. and Cranor, L.F. (2005) *Privacy Indexes: A Survey of Westin's Studies*.

Li, D. (2010) 'Privacy protection in social networking services', *T-110.5290 Seminar on Network Security*, Aalto University.

Lind, P.G., da Silva, L.R., Andrade, J.S. Jr. and Herrmann, H.J. (2007) 'Spreading gossip in social networks', *Physical Review E*, Vol. 76, No. 3, p.036117.

Liu, K. and Terzi, E. (2009) 'A framework for computing the privacy scores of users in online social networks', *Data Mining, 2009: ICDM'09: Ninth IEEE International Conference on*, pp.288–297, IEEE.

Liu, K., Das, K., Grandison, T. and Kargupta, H. (2008) 'Privacy-preserving data analysis on graphs and social networks', *Next Generation Data Mining*, CRC Press.

Liu, Y., Gummadi, K.P., Krishnamurthy, B. and Mislove, A. (2011) 'Analyzing Facebook privacy settings: user expectations vs. reality', *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference*, pp.61–70, ACM.

Mazzia, A., LeFevre, K. and Adar, E. (2012) 'The PViz comprehension tool for social network privacy settings', *Proceedings of the Eighth Symposium on Usable Privacy and Security*, p.13, ACM.

Palen, L. and Dourish, P. (2003) 'Unpacking privacy for a networked world', *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp.129–136, ACM.

Papacharissi, Z. and Gibson, P.L. (2011) 'Fifteen minutes of privacy: privacy, sociality, and publicity on social network sites', *Privacy Online*, pp.75–89, Springer.

Petronio, S.S. (2002) *Boundaries of Privacy*, State University of New York Press Albany, NY.

Shaw, A.K., Tsvetkova, M. and Daneshvar, R. (2011) 'The effect of gossip on social networks', *Complexity*, Vol. 16, No. 4, pp.39–47.

Shen, Y. and Pearson, S. (2011) *Privacy Enhancing Technologies: A Review*, HPL-2011-113 [online] http://www.hpl.hp.com/techreports/2011/HPL-2011-113.html.

Sleeper, M., Balebako, R., Das, S., McConahy, A.L., Wiese, J. and Cranor, L.F. (2013) 'The post that wasn't: exploring self-censorship on Facebook', *Proceedings of the 2013 Conference on Computer Supported Cooperative Work*, pp.793–802, ACM.

Solove, D.J. (2006) 'A taxonomy of privacy', *University of Pennsylvania Law Review*, Vol. 154, No. 3, pp.477–560.

Srivastava, A. and Geethakumari, G. (2013) 'A framework to customize privacy settings of online social network users', *Intelligent Computational Systems (RAICS), 2013 IEEE Recent Advances in*, pp.187–192, IEEE.

Stutzman, F. and Kramer-Duffield, J. (2010) 'Friends only: examining a privacy-enhancing behavior in Facebook', *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp.1553–1562, ACM.

Toch, E., Wang, Y. and Cranor, L.F. (2012) 'Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems', *User Modeling and User-Adapted Interaction*, Vol. 22, Nos. 1–2, pp.203–220.

Trepte, S. and Reinecke, L. (2011) 'The social web as a shelter for privacy and authentic living', *Privacy Online*, pp.61–73, Springer.

Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P.G. and Cranor, L.F. (2011) 'I regretted the minute I pressed share: a qualitative study of regrets on Facebook', *Proceedings of the Seventh Symposium on Usable Privacy and Security*, p.10, ACM.

Warren, S.D. and Brandeis, L.D. (1890) 'The right to privacy', *Harvard Law Review*, Vol. 4, No. 5, pp.193–220.

Westin, A.F. and Blom-Cooper, L. (1970) *Privacy and Freedom*, Vol. 67, Atheneum, New York.

Wu, X., Ying, X., Liu, K. and Chen, L. (2010) 'A survey of privacy-preservation of graphs and social networks', *Managing and Mining Graph Data*, pp.421–453, Springer.

Yildiz, H. and Kruegel, C. (2012) 'Detecting social cliques for automated privacy control in online social networks', *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on*, pp.353–359, IEEE.