2015 IEEE International Conference on Smart City/SocialCom/SustainCom together with DataCom 2015 and SC2 2015

Privacy preserving information dispersal in social networks based on disposition to privacy

Vidyalakshmi B. S.
School of Computer Science & Engineering
University of New South Wales
Sydney, Australia
v.vidyalakshmi@student.unsw.edu.au

Raymond K. Wong
National ICT Australia and
University of New South Wales
Sydney, Australia
wong@cse.unsw.edu.au

Chi-Hung Chi
Computational Informatics
CSIRO
Tasmania, Australia
chihung.chi@csiro.au

***Abstract*—Social networks are no more a phenomenon. They have assimilated into our daily lives and are a part of our being. It has become a vehicle that carries information on our triumphs, failures, social and societal views, travel and leisure activities. Information shared through social networks contain sensitive information that poses a serious threat to our privacy. One of the contributing factor in being victimised is, information reaching more than the intended audience. Ignorance towards risk posed, sheer neglect towards privacy or complexity in understanding the privacy settings are pushing the general public in the direction of privacy breaches. We address controlling the intended audience for the information posted on social networks in this work on privacy. The notion of disposition to privacy of the user in assessing his friends, has not been strongly addressed before. We propose a model for quantifying privacy where the user's disposition (personality) towards privacy decides which information is seen by whom. Access to information is driven through assigning visibility to groups of users, traditionally. We propose to shift this access control to category. Category is a virtual container of information; profile items and general posts included. By this shift, we contend that information privacy is intuitive and hassle free from end users perspective thereby assisting to have a tight control over sensitive information.**

I. Introduction

Social networking sites provide a distinct platform to build social relations among people who share common interests and activities, common background or who are known to us offline [21]. Users create profile describing themselves and share their ideas, photos, experiences, events and activities with their network of friends.

Any system, be it information retrieval, social network, query or resource allocation, needs information about the users of the system in order to define strategies and intentions of the users. Similarly, the users need information about the users of the system and the system as a whole [2]. This calls for sensitive information to be disclosed by the user, to the system, in order to establish user identity, measure users intentions and satisfaction.

Often users willingly disclose personal information. The reasons for users' information disclosure on social networks has been an active area of research [4] [23] [9]. Major factors influencing information revelation were found to be future audiences, general privacy concerns and gender [23]. Also, users discern personal information revelation as necessary to make the social networks useful, *Why have a profile if your profile doesnot say enough about who you are?* [23] [9]. Age, Sex, Political orientation, Place of birth, Mothers' maiden name are some such sensitive information [4] revealed over social networks. While information disclosure is important for the functioning of social networking, it also carries a significant privacy risk. Privacy can be at risk due to wilful disclosure of personal information due to a number of factors ranging from peer pressure, ignorance, trust in social network service providers and its members, neglect in assessment of risks vs benefits or lazy attitude towards privacy [9].

The problem is not so much in disclosing personal information but much to do with who the intended audience are. Most of the online social networks provide functionality to set visibility to each of the profile items, so also for the information being shared through posts. FOAF (Friend of a friend) is one of most common paradigm used for setting visibility [1]. FOAF information sharing is not always intuitive. Grouping of friends has been introduced as an alternative to FOAF by the social networking services. Users tend to have groups for information disbursement, such as *Work Mates*, *Family*, *Close Friends*, *Acquaintances*. Grouping through lists (automatic as in Facebook), circles (manually created in Google+), lists (manually created as in Twitter) often leads to friends overlapping multiple groups with users finding the grouping to be noisy, hard and rigid [12]. Users are left with the choice to create and manage the groups over time or take the easy route of disbursing information to all, there by ending up sharing information to more people than intended to.

In this paper, as an alternative to group based information dispersal, we propose to disperse information through information categories. Categorisation is based on the sensitivity of information shared. We contend that, information sharing would be more organised and manageable if the information shared in the past and the information being shared in the present was grouped into categories and user is given a choice to set the privacy level required, to access these information. To access the information housed inside categories, users friends are evaluated for their privacy affinity towards users' information and assigned a value for privacy score, Privacy Affinity Value (PAV). Different PAV values give access to different categories of information.

We propose to use *disposition to privacy* of the user in deciding the privacy score or Privacy Affinity Value (PAV) of the friends. Disposition to privacy is the inherent nature of an individual towards the notion of privacy when disclosing

978-1-5090-1893-2/15 $31.00 © 2015 IEEE
DOI 10.1109/SmartCity.2015.100

information to others in his social circle. This disposition is not towards an individual but is the stable non-changing personality or attitude of a user towards all individuals he encounters. *How privacy oriented is the user?* is a question that answers users' disposition to privacy. It is intuitive for a user to answer a question - *Do you trust friend f_1 more than friend f_2 with your information?*. It is this intuitiveness that we make use of. As the first step, the sorted array of friends of the user are assigned positions $\{f_1, f_2\}$, based on their privacy affinity towards users' information. These positional values in the sorted array is used as input to bezier curve, a function that is used to calculate the PAV values of the friends of the user in the second step. Bezier curve is an approximation curve that is extensively used in the field of computer graphics, animations and automobile design among others. In this paper, we use the quadratic form of the bezier curve. Summarizing our contributions -

- We propose a category based information dispersal as an alternative to group based information dispersal in social networks
- We adopt bezier curve as a friend evaluation and scoring function to arrive at a non-changing PAV value of each friend in the users' network. This can be used to control visibility to categories of information including profile information, posts, comments to posts.
- We propose several dimensions of information that can be used to assist user in pre-sorting his friends to arrive at a sorted list of friends.

Rest of the paper is organized as follows – Section II gives related work, while Section III explains the concept of disposition to privacy, Section IV describes the proposed model, Section V describes categorisation and access control of information, Section VI outlines the algorithm and Section VII concludes along with describing scope for future work.

II. Related Work

We review works that consider privacy scoring as a measurement of privacy of users in social networks along with works that consider grouping of information as an alternative to grouping of users.

A framework based on Item Response Theory (IRT) has been proposed by [17] in which a user's privacy score can be calculated by scoring the sensitivity of the profile item and visibility it gets in an OSN network. The work arrives at a privacy score for each user using this framework. We consider this work as important albeit orthogonal to the framework we suggest, as we propose to use the privacy score in setting visibility for not only the profile items but also the general information shared on the OSN, such as posts, tags, comments.

Grouping information revealed on an OSN, to identify the smallest group of information that users need, to perform specific interactions in an OSN, is proposed in [16]. They group the bits of information into thumbnail, greater profile, list of friends, user generated content and comments and try to find the smallest group from among these. We share the same approach of grouping of information. But, differ in the fact that we group the information based on sensitivity of information and not on what the information is about (context).

Privacy quotient and *Privacy Armor* models [20] are proposed as a way to measure privacy leaks using the IRT model. The authors identify the importance of posts, tweets and other unstructured information that are the sources of privacy leakage. Privacy Armor model proposed, measures average privacy quotient of the group members, who would be probable audience of a message about to be posted. If the score does not meet the desired score, user is alerted and can take appropriate steps. While using posts, tweets and other unstructured data, information is classified as sensitive and not-sensitive based on the presence of profile items alone thereby restricting the leakages to 11 profile items discussed in the paper.

Privacy Index (PIDX) proposed [18], is a measure of a user's privacy exposure in a social network. PIDX is a numerical value between 0 and 100 with high value indicating high privacy risk in social networks. PIDX is the summation of privacy impact factors of each attribute visible where in each attributes privacy impact factor is the ratio of its privacy impact to full privacy disclosure. Extending the PIDX model, the authors have proposed [25], which measures the privacy exposure between any two given users i and j, $PIDX(i, j)$. The paper does not clearly mention the methods used for deep web searching and data aggregation. Also, the backbone of the proposed Privacy Index, the privacy impact factor is a static measure focusing on few attributes listed in the paper.

Privacy scoring using bezier curve has been proposed by [24]. Bezier curve in its cubic form is used as it has to account for both privacy orientation and communication orientation of the user, while we use the quadratic form of bezier curve in this paper to arrive at privacy scores for friends. We use the communication information for pre-sorting of friends which is lacking in [24].

All the above papers apart from [24] arrive at friends' privacy score using the information user has disclosed to his friends. Different than these papers, in this paper we propose to estimate privacy scores of friends from the user's perspective utilising user's disposition to privacy.

III. Disposition to Privacy

Consider a friend Tom who is Harry and Beth's friend on a social network. Harry thinks Tom is very privacy oriented and so does Beth. Tom behaves the same way with both Harry and Beth. Harry assigns Tom a value of 8 out of 10. But, Beth assigns him a 5 out of possible 10 as privacy value. In this situation, Harry is less privacy oriented than Beth and hence the varying weightages assigned. There is a need to account for this personality of the users (Harry and Beth) in quantifying privacy ratings to their friends.

Attitude of the user towards privacy should be considered, in deciding, from among his friends, whom the user considers privacy oriented and entitled to receive sensitive personal information, from him, through social networks. A user may himself be more or less privacy oriented.

IV. Proposed Model

A. Preliminaries

Privacy in social networks has been evaluated by [5] [22] [8] [7]. Privacy value ranges adopted are from 0 to 1 or 1

to 10. A different paradigm proposed in [14] [13] consider the subjectivity of privacy of each user in the model as uncertainty, and represent privacy value in a multi-dimensional model. Yet another approach adopted is to divide privacy into strata, and assign them qualitative labels. In this paper, we rest the ability to fix the range with the user. We propose to address subjectivity of privacy also known as disposition to privacy as maximum privacy attainable (0 is maximum score) to maximum information disclosure threshold (PT^0) that the user can tolerate (> 0). Each user is free to define his threshold value and evaluate his friends' privacy orientation or privacy affinity according to the defined scale.

The social network of a user can be represented as a directed graph and the relationship between the user and his friend can be represented as an edge e. The direction of representation in the graph's edge is from the user who is evaluating his friend's privacy affinity $user \xrightarrow{e} friend$. $P_g(N, E)$ represents a directed graph such that N represents the number of friends, E represents the set of relations formed by the set of edges e.

In a peer-to-peer communication setting, [19] have proposed a way to address the disposition to trust. The model considers users' disposition to trust as a value between 0 and 1, with 0 representing most trustful behavior and 1 representing the most distrustful behavior. By accounting for users' disposition to trust, peers are assigned quantified trust values using bezier curve to arrive at these values. Trust and Privacy are shown to enhance each other as well as act in a compensatory manner with respect to each other [4] [11] [3]. Given that trust and privacy are closely related and have been studied together in the area of social networks, we propose to use the model by Saadi. et. all [19] and adopt it to arrive at a quantified privacy value.

Fig. 1 gives a detailed architecture of the different steps involved in arriving at a privacy score, the PAV value. Friends are sorted in the privacy sort module and fed as input to the PAV calculation module. Information is categorised in categorisation module, access control to categories using PAV value is handled through the access control module. We explain each of the modules in detail, in the following sections.

B. PrivacySort

Example : Consider a situation where Harry and Beth have to rate Tom and Jill, their only two friends in a given social network. Tom and Jill show similar behaviors while interacting with Harry and Beth and Harry and Beth's personal information. Harry rates Jill to be more privacy oriented than Tom. Beth, is likely to rate similarly. Using proposed PrivacySort, both would rate privacy orientation of Jill higher than that of Tom and this is reflected in the sorted list of friends, sorted after answering the question *who is more privacy oriented with your data, Jill or Tom?*. It's important to note that though, Harry and Beth may have different privacy orientation (disposition), their sorted list of friends would look same. This alternate approach is very likely to have consistent results rather than user assigning friends privacy scores directly.

It is intuitive to compare friends with each other to judge who is more privacy oriented than whom. PrivacySort aims to arrive at a sorted list of friends, sorted based on their affinity

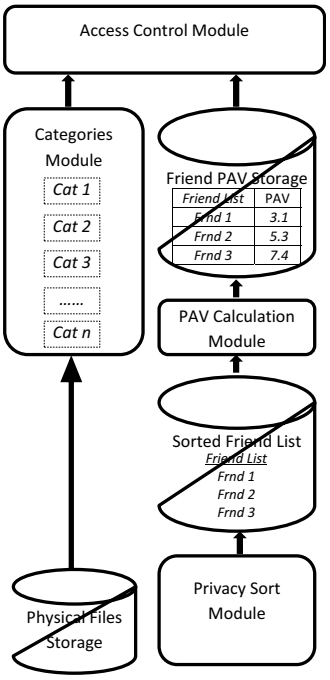

Fig. 1. Architecture Diagram

to privacy, as perceived by the user. The notion of evaluating one friend with respect to the other for their privacy affinity is termed as *PrivacySort*.

Definition - Given a user u and his friend f_i in a social network, there exists a direct relation represented by an edge e where ($f_i \in N$). Privacy set $PS = f_1, f_2, ...f_N$ is a set of sorted friends list, with their positions indicating the privacy affinity as perceived by the user. PrivacySort (f_1) = 1 and PrivacySort(f_2) = 2 means that user perceives friend f_1 to be more privacy oriented than friend f_2.

As the number of friends in a user's network keeps on increasing, comparison of friends with each other, to assess privacy affinity, starts becoming difficult. We propose to use some of the on-demand grouping methods and frameworks [26], [15], [6], proposed for grouping friends in social networks, as a starting point for PrivacySort. They can be used in place of manual sorting of friends to come up with a pre-sorted friends list which can be modified by the user to come up with a sorted list of friends. Some of the pre-sorting methods that can be used are as follows:

- Tie-strength - [6], [26] propose to use both profile attributes information and communication information of user and his friends, in calculating tie-strength. This can be used to pre-sort the users' friends. Tie-strength offers the concept of user being strongly connected to some of his friends while weakly connected to others.
- Communication information - [15] propose to use only communication information in finding the tie-strength. This method can be used for pre-sorting in cases where attribute information is left unfilled or for social networks where profile attribute information is not compulsory (eg., Twitter)
- Number of mutual friends - [10] have shown a simple

measure like mutual friends to be correlated with complex measurements to find the Tie-strength between user and his friends. This measure, available on most social networks, could be used for pre-sorting of friends.

C. Behavior function

Behavior function (BV) represents a curve in the cartesian coordinate system. Bezier curve is used to implement the BV function due to the flexibility it offers in plotting geometric curves. We choose quadratic bezier curve to calculate the privacy score. Bezier curves are defined by the control points that controls the shape of the curve. By fixing the start and the end points and choosing the control points, we can adjust the curvature of the curve. A quadratic bezier curve has one control point which accounts for the disposition to privacy of user, in this paper.

Bezier curve is expressed in parametric form to draw a smooth curve. The points are represented by $P_0, P_1 ... P_n$ with P_0 being the starting and P_n being the end point. With a quadratic bezier curve we have P_0, the starting point, P_1, the control point, and P_2, the threshold point.

To draw the bezier curve, input is x, a positive number representing the position of the friend in the list of N friends. The output of the PrivacySort gives the position number, with friend in position 1 representing the highest privacy affinity node and friend at N representing the lowest privacy affinity node, as perceived by the user.

The bezier curve is plotted by considering the position number as the abscissa x and returning quantitative trust value $BV(x)$. Quadratic bezier curve is drawn by taking input, a temporal variable t, to obtain output as points corresponding to abscissa and ordinate. To suit the needs of behavior function $BV(x)$, the ordinate is obtained as a function of abscissa.

The three points required to draw the bezier curve to suit the needs of behavior function are -

- The origin point $P_0(0, 0)$
- The behavior point $P_1(b_x, b_y)$
- The threshold point $P_2(h_x, h_y)$

h_x represents the number of sorted nodes (friends) and h_y is given by the privacy threshold PT^0. The bezier curve is drawn using the three points and the assumption is that it is sufficient to move the point P_1 through the second diagonal of the defined rectangle $b_x = \frac{-h_y}{h_x} * b_y + h_y$ to plot a large panel of behaviors of the user from being extremely privacy conscious $P_1(0, h_y)$, to least privacy concerned $P_1(h_x, 0)$. Position of point P_1 is fixed according to disposition to privacy l^0. BV function is defined as in [19]:

$$\begin{aligned} BV : [0, h_x] &\rightarrow [0, h_y] \\ X &\rightarrow Y \end{aligned}$$

$$BV_{l^0,h_x,h_y}(X) =$$

$$\begin{cases} \frac{(h_y - 2b_y)}{4b_x^2})X^2 + \frac{b_y}{b_x}X & if(h_x - 2b_x = 0) \\ (h_y - 2b_y)(\propto (X))^2 + 2b_y \propto (X) & if(h_x - 2b_x \neq 0) \end{cases}$$

$$where \begin{cases} \propto (X) = \frac{-b_x + \sqrt{b_x^2 - 2b_x * X + h_x * X}}{h_x - 2b_x} \\ 0 \leq b_x \leq h_x \ and \ h_x > 0 \\ b_x = (1 - l^0).h_x \ and \ b_y = h_y.l^0 \end{cases}$$

Disposition to privacy is expressed as a value between 0 and 1 and is represented by variable l^0. Low disposition to privacy can be represented as $l^0 = 0$ and highest disposition to privacy can be represented as $l^0 = 1$. Higher disposition to privacy indicates that the user believes the risk to his information at the hands of his friend is higher and hence assigns values nearer to privacy threshold PT^0. We will explain why the most privacy oriented friend i.e., the friend with PrivacySort position 1, will be able to access most sensitive information of the user in Section V.

D. Quantifying Privacy Affinity Value (PAV)

User is free to fix his disposition to privacy, l^0, as a value between 0 and 1, say l^0 = 0.8. He is also free to fix the range of values starting from 0 to PT^0, with $PT^0 > 0$. After evaluating the behavior function $BV(x)$ for all the edges e (formed by the direct link between the user and his friend), we get Privacy Affinity Value (PAV) of each friend in the network. The friends are plotted along the abscissa of the bezier curve, in the same order as obtained through PrivacySort. The ordinate is the quantified PAV. Evaluating:

$$PAV(U, f_i) = BV_{l^0,h_x,h_y}(PrivacySort(f_i))$$

where,

$P_1 = l^0$	$\mid 0 < l^0 < 1$
$P_2 = (h_x, h_y)$	$\mid h_x =$(Number of friends + 1)
$h_y = PT^0$	$\mid$ (The privacy threshold)

Lower the PAV value (away from PT^0), more the privacy orientation of the user's friend (f_i), towards users' (U) information, and, higher the PAV value of a friend, lower is his privacy orientation.

Let us consider a sample PAV allocation as in Table 1. User's friends (f_1, f_2, f_3, f_4) are evaluated for their privacy affinity by the user using PrivacySort and Behavior functions. Friend f_1 is more privacy oriented than f_4. Friend f_4 is more privacy oriented than f_3 with friends f_2 having the lowest privacy affinity.

Sorted Friends	f_1	f_4	f_3	f_2
PAV	3.1	5.3	7.4	8.5

TABLE 1
SAMPLE PAV OF FRIENDS (f_1, f_2, f_3, f_4)

V. CATEGORISATION AND ACCESS CONTROL

Categories can be considered as virtual containers of the information. Information can be profile items or general posts. To highlight the need of categorisation of information in a social network, we give two scenarios.

• The current working from a popular social network, Facebook, highlights the presence of functionality similar

to categorisation and its usefulness. Facebook provides the functionality to group photos into an album and set the visibility of the album as a whole either to a single person or a group of people. This is because the whole album is having similar content and can thus be grouped together and its visibility controlled as a whole. This functionality if not available for grouping of general information; be it posts or profile information. We propose to provide the functionality to group any information being shared on social networks. By grouping information based on the sensitivity of information into categories, it will align with the concept of privacy.

• Traditionally, user's friends are grouped based on their social relation (eg., Family, Close Friends, Acquaintance) or context of their relationship (eg., Work Mates, Soccer Teammates). This kind of grouping does not address a situation where user would like to share information on for example *being demoted at work due to restructure* with siblings, parents and selected close friends only, due to privacy concerns. Existing solution is to create a group with siblings, parents and selected close friends and set visibility on this information. Creating groups in small numbers is manageable, but, as the number of groups increase management is cumbersome. Hence, information dispersal through categories is better than through friends groups as privacy of information is an important motivation behind information dispersal through categories.

A. Information Categorisation

Information allocation to categories is disjoint i.e., a piece of information belongs to exactly one category. The weight or maximum PAV assigned to categories convey the PAV range that they can accept, to provide access to the information housed. Let Cat_w indicate the maximum PAV range of a category beyond which access to the category is denied. It is calculated as -

$$Cat_w = (\frac{R_{cat}}{Num_{cat}}) \cdot PT^0$$

where R_{cat} is the ranking of the category after hierarchically arranging the categories based on information sensitivity. Lower the ranking, higher the sensitivity of information housed. Num_{cat} denotes the total number of categories, PT^0 is the privacy threshold.

Example: Let privacy threshold be $PT^0 = 10$. In Table 2, information is categorised into 3 categories. The max PAV to access a category is given by Cat_w. This value can also be adjusted by the user to suit the needs of privacy. A friend f_1, as in Table 1 with a PAV value of 3.1 can essentially access all the categories in Table 2. It is also important to note that the user can override the calculated Cat_w as shown in Table 2, column $Adjusted\ Cat_w$

B. Access Control

Access to information in categories of user U by the friend f_i is based on the $PAV(U, f_i)$. Categories are assigned the category weight Cat_w which denotes the max PAV value tolerated to access a category. After calculation of friends PAV and fixing the Cat_w of the categories, access control assignment to all friends, is completed.

Category	R_{cat}	Cat_w	Adjusted Cat_w
Personal	1	3.3	3.5
Controlled	2	6.6	6
General	3	10	9

TABLE 2
EXAMPLE CATEGORY SET

Example: Let us consider the categories as in Table 2 with their weights defined and consider the PAV values as defined in Table 1 for the analysis of access control. Friend f_1 is the most privacy oriented and has the highest PAV, whereas, friend f_2 is the least privacy oriented and has low PAV. f_1 can access information from categories *personal, controlled* and *general* as his PAV is 3.1 and the requisite PAV for category *personal* is ($<$3.5), for *controlled* is ($<$6) and for *general* is ($<$9) . Friend f_2 can access information from only *general* Category.

We contend that the model is flexible in handling many situations encountered in social networks. Let us analyse a few scenarios to understand the flexibility of the proposed model.

Case 1: A friend is demoted in the PrivacySort due to him indulging in distribution of sensitive information of the user. Since his current position dictates his visibility for past and future information shared by the user, visibility control is clear. Traditionally, by using groups to control visibility, the friend had to be removed from all the groups which had access to information or has to be added to a group created specifically to curtail the visibility of information for the friend. Alternatively, the user can be blocked all together. To downgrade his access without blocking the access altogether is tedious.

Case 2: A new friend is added to the friends list. The friend is assigned a position in the sorted list of friends indicating his privacy affinity as perceived by the user. This automatically grants him access to past and present information of the user without him having to be added into groups, as done traditionally, to view information from the user.

Case 3: Change in user's disposition to privacy. We have opined earlier that disposition to privacy is stable non-changing personality of a user towards all individuals he encounters. We also note that the disposition to privacy of a user develops as a result of situations he encounters and the actions he takes to counter the privacy risks faced in those situations. This trait of the user can change over time due to positive or negative experiences he undergoes. Hence, we note that a user's disposition to privacy can change over time. Once user's disposition to privacy changes, he can adjust the l^0, essentially recalculating PAV for all his friends and adjust the category weights Cat_w.

By classifying the information into categories, we argue that long-term control of information is feasible.

VI. ALGORITHM

A. Algorithm 1: PAV calculation for User's friends

This algorithm is to derive PAV value of each friend in User's friends list. l^0 is set a value between 0 and 1, signifying user's disposition to privacy. PT^0 is the threshold privacy tolerance of a user. Friends list is sorted through function

Algorithm 1 PAV calculation

$Initialize \quad l^0$;
$Initialize \quad PT^0$;

$InitializeFriendlist[i] = (f_1, f_2, ..., f_N)$
$NumOfFriends = Sizeof(Friendlist[i])$
for each do $FriendList[i]$ ▷ *Sort all the friends*
    $SortedArray[j]$ = $PrivacySort(Friendlist[i])$
end for
for each do $SortedArray[j]$ ▷ *for each friend in the SortedArray[j], calculate BV()*
    $BV_{l^0,NumOfFriends+1,PT^0}$
end for
$Call \quad AccessControlProcedure$

PrivacySort to yield a SortedArray of friends, sorted based on their privacy affinity as perceived by the user. The Behavior function $BV()$ calculates the Quantified Privacy Value (PAV). The PAV thus calculated is referred as and when there is a access request from user's friend on user's information. This algorithm is rerun only when the friend moves down or up in the privacy orientation towards user's data or when there is an addition or deletion of friend.

VII. Conclusion and Future Work

In this paper, we have proposed a privacy control framework for information dispersal on social network. We have considered user's disposition to privacy as the driving factor in quantifying privacy values (PAV) of user's friends. The PAV values control access to information through categories. Categories are virtual containers housing information of similar sensitivity or privacy requirements. By assigning privacy value range up to which a category can be accessed, friends with similar privacy affinity behavior get access to same categories. By shifting the visibility control of information from being done through groups to categories, new information can be automatically directed at the right user. There is no need to set visibility for each information shared as it is controlled at a much higher level, namely, categories. By controlling access to information through categories, we argue that privacy is enhanced by simplifying visibility control of information. As future work, we would like to test the framework on social network datasets. We would also like to test proposed presorting techniques in the PrivacySort.

References

[1] D. Brickley and L. Miller. FOAF vocabulary specification. Namespace Document, FOAF project, 2004.

[2] Y. Busnel, P. Serrano-Alvarado, and P. Lamarre. Trust your social network according to satisfaction, reputation and privacy. In *Proceedings of the Third International Workshop on Reliability, Availability, and Security*, page 6. ACM, 2010.

[3] C. Dwyer, S. R. Hiltz, and K. Passerini. Trust and privacy concern within social networking sites: A comparison of facebook and myspace. In *Americas Conference on Information Systems*, page 339, 2007.

[4] M. Faisal and A. Alsumait. Social network privacy and trust concerns. In *Proceedings of the 13th International Conference on Information Integration and Web-based Applications and Services*, pages 416–419. ACM, 2011.

[5] D. Gambetta. Can we trust trust. *Trust: Making and breaking cooperative relations, electronic edition, Department of Sociology, University of Oxford*, pages 213–237, 2000.

[6] E. Gilbert and K. Karahalios. Predicting tie strength with social media. In *Proceedings of the Conference on Human Factors in Computing Systems*, pages 211–220. ACM, 2009.

[7] J. Golbeck and J. Hendler. Filmtrust: Movie recommendations using trust in web-based social networks. In *Proceedings of the IEEE Consumer communications and networking conference*, volume 96, 2006.

[8] N. Griffiths. Task delegation using experience-based multi-dimensional trust. In *Proceedings of the fourth international joint conference on Autonomous agents and multiagent systems*, pages 489–496, New York, NY, USA, 2005. ACM.

[9] R. Gross and A. Acquisti. Information revelation and privacy in online social networks. In *Proceedings of the 2005 workshop on Privacy in the electronic society*, pages 71–80. ACM, 2005.

[10] M. Gupte and T. Eliassi-Rad. Measuring tie strength in implicit social networks. In *Proceedings of the 4th Annual Web Science Conference*, pages 109–118. ACM, 2012.

[11] A. N. Joinson, U.-D. Reips, T. Buchanan, and C. B. P. Schofield. Privacy, trust, and self-disclosure online. *Human–Computer Interaction*, pages 1–24, 2010.

[12] S. Jones and E. O'Neill. Feasibility of structural network clustering for group-based privacy control in social networks. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, page 9. ACM, 2010.

[13] A. Jøsang, R. Hayward, and S. Pope. Trust network analysis with subjective logic. In *Proceedings of the 29th Australasian Computer Science Conference*, pages 85–94, 2006.

[14] A. Jøsang and S. Pope. Semantic constraints for trust transitivity. In *Proceedings of the 2nd Asia-Pacific conference on Conceptual modelling*, pages 59–68. Australian Computer Society, Inc., 2005.

[15] I. Kahanda and J. Neville. Using transactional information to predict link strength in online social networks. *International AAAI Conference on Web and Social Media*, pages 74–81, 2009.

[16] B. Krishnamurthy and C. E. Wills. Characterizing privacy in online social networks. In *Proceedings of the first workshop on Online social networks*, pages 37–42. ACM, 2008.

[17] K. Liu and E. Terzi. A framework for computing the privacy scores of users in online social networks. *ACM Transactions on Knowledge Discovery from Data*, 5(1):6, 2010.

[18] R. K. Nepali and Y. Wang. Sonet: A social network model for privacy monitoring and ranking. In *IEEE 33rd International Conference on Distributed Computing Systems Workshops*, pages 162–166, 2013.

[19] R. Saadi, J.-M. Pierson, and L. Brunie. T2d: A peer to peer trust management system based on disposition to trust. In *Proceedings of the 2010 Symposium on Applied Computing*, pages 1472–1478. ACM, 2010.

[20] A. Srivastava and G. Geethakumari. Measuring privacy leaks in online social networks. In *International Conference on Advances in Computing, Communications and Informatics*, pages 2095–2100. IEEE, 2013.

[21] K. Subrahmanyam, S. M. Reich, N. Waechter, and G. Espinoza. Online and offline social networks: Use of social networking sites by emerging adults. *Journal of Applied Developmental Psychology*, pages 420–433, 2008.

[22] S. Toivonen, G. Lenzini, and I. Uusitalo. Context-aware trust evaluation functions for dynamic reconfigurable systems. In *Workshop on Models of Trust for the Web*, 2006.

[23] Z. Tufekci. Can you see me now? audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, pages 20–36, 2008.

[24] B. Vidyalakshmi, R. K. Wong, and C.-H. Chi. Privacy scoring of social network users as a service. In *IEEE International Conference on Services Computing*, pages 218–225, 2015.

[25] Y. Wang, R. K. Nepali, and J. Nikolai. Social network privacy measurement and simulation. In *International Conference on Computing, Networking and Communications*, pages 802–806. IEEE, 2014.

[26] R. Xiang, J. Neville, and M. Rogati. Modeling relationship strength in online social networks. In *Proceedings of the 19th international conference on World wide web*, pages 981–990. ACM, 2010.