2014 IEEE International Conference on Services Computing

Privacy as a service in social network communications

Vidyalakshmi B. S.
University of New South Wales
Sydney, Australia

Raymond K. Wong
University of New South Wales
and National ICT Australia

Mojgan Ghanavati
University of New South Wales
and National ICT Australia

Chi-Hung Chi
CSIRO
Tasmania, Australia

***Abstract*—With dispersing of information on social networks - both personally identifiable and general - comes the risk of these information falling into wrong hands. Users are burdened with setting privacy of multiple social networks, each with growing number of privacy settings. Exponential growth of applications (App) running on social networks have made privacy control increasingly difficult. This necessitates Privacy as a service model, especially for social networks, to handle privacy across multiple applications and platforms. Privacy aware information dispersal involves knowing who is receiving what information of ours. Our proposed service employs a supervised learning model to assist user in spotting unintended audience for a post. Different from previous work, we combine both Tie-strength and Context of the information as features in learning. Our evaluation using several classification techniques shows that the proposed method is effective and better than methods using either only Tie-strength or only Context of the information for classification.**

I. Introduction

Software as a service (SaaS), Infrastructure as a service (IaaS), Platform as a service (PaaS), Backend as a service (BaaS), Information technology management as a service (ITMaaS) are some of the services gaining ground. *Privacy as a service* is another such viable model. With our ever increasing online presence, Privacy as a service[1] [10], [16] has drawn the attention of researchers and companies alike due to the urgency of the matter, especially in the context of privacy breaches heard every now and then.

Our online identity is being increasingly defined by social networks identities. With social networking sites increasing popularity (1.23 billion monthly active users for Facebook[2], 540 million active users on Google+ each month[3]), their use is becoming the norm and has necessitated identity management, access control and encryption mechanisms. Increased desire to become popular, aided by lazy and careless attitude towards privacy [3], [8], [31] has seen a marked increase in disclosure of personal information and opinions online, leading to privacy being at the receiving end.

Examples of over-sharing on social networks, leading to being sacked from jobs[4], irreversible damage to personal relations[5] are surfacing frequently. Embarrassing situations, Blackmailing, Identity theft are some of the troublesome offshoots of information reaching more than the intended audience [8], [23].

Problem is not so much in disclosing information on social networks, but, has much to do with who the intended audience are. Finding the intended audience can be seen as privacy-aware group creation problem.

Current social networks recommend to pre-classify friends into groups and to use these groups for communication. Available social network features like Circles from Google+[6], pre-defined group (Lists in Facebook terminology) based communication from Facebook leave the responsibility of Circles and group creation on users, which is not desirable. Smartlists[7] from Facebook try to answer this shortcoming by automatic creation of lists based on common features, social graph or inferred information and these groups can be edited by the user for correctness. But, they are shown to be ineffective due to being rigid, noisy and problematic in managing security [11]. Hence, pre-defined groups, Circles or Smartlists may not be sufficient to answer all the information sharing needs.

Research in this regard has shown a need for in-context, on-demand group creation [1] as willingness to share varies not only on content recipients but also on content itself [21]. The underlying contexts of friendship are an important indicator of what information user and his friend share. Information, belonging to one context, may be appropriate to a *close friend* (eg., Friends can be added to a *close friends* list in Facebook). Given another piece of information belonging to a different context, may not be suitable for the same *close friend* as they may not share the context of next information. Here, the definition of *close friend* is relative to the contexts they share in friendship. Hence, it is important that the context of the information posted should be shared by recipients of the information. Clearly, there is a need to disperse information with enough weightage given to context of information and the underlying contexts of friendship.

All friends who share a context may not share the same intensity of friendship. Sharing of context attributes do not warrant information to be shared with all of them. A neighbor, school friend, colleague may share certain context defining attributes (eg., location). But, they may be mere *acquaintance* rather than a friend. Social network treats all connections

[1]http://www.computerworld.com/s/article/9236404/Security-as-a-service-gaining-popularity

[2]http://investor.fb.com/releasedetail.cfm?ReleaseID=821954

[3]http://googleblog.blogspot.com.au/2013/10/google-hangouts-and-photos-save-some.html

[4]http://edition.cnn.com/2013/06/06/living/buzzfeed-social-media-fired

[5]http://www.nydailynews.com/life-style/facebook-ruining-marriage-social-network-named-divorce-filings-2011-article-1.1083913

[6]http://www.nytimes.com/2011/07/14/technology/personaltech/google-gets-a-leg-up-on-facebook.html

[7]https://www.facebook.com/notes/facebook/improved-friend-lists/10150278932602131

978-1-4799-5066-9/14 $31.00 © 2014 IEEE
DOI 10.1109/SCC.2014.67

IEEE computer society

as friends and since contexts shared between users, cannot differentiate a *friend* from an *acquaintance*, there is a need for a measure, of friendship. Tie-strength, in social networks, determines the strength of a friendship through measuring the similarity between their profile items and communication [6], [29], [32].

Making use of both Context of information and Tie-strength, this paper proposes a service-oriented supervised learning model to assist user in determining the right target audience for each post about to be posted. Privacy aware information dispersal involves assisting user in understanding, from among his friends, who match the learnt model and who do not. The service considers profile similarity and communication intensity and recency, used in tie-strength determination, as features that are used in supervised learning. The privacy service solicits user response in identifying the context defining attributes of information about to be posted as the user is the best judge in identifying the underlying context of the information. Here, *Context* is a composite attribute made up of one or more context defining attributes.

Our contributions can be summarized as follows:

- A new approach to privacy aware information dispersing, utilising machine learning on user data for classification.
- To the best of our knowledge, this is the first attempt in using Context and Tie-strength together in determining the intended audience of a post.
- An evaluation of the effectiveness of the proposed method against classification based on Tie-strength alone or classification based on Context alone.

The rest of the paper is organised as follows. We compare our work to the existing work in section II, in section III, we explain the background and motivation to our model. Details of the proposed model, along with framework and service implementation details are given in section IV. We demonstrate the effectiveness of the proposed model using Facebook dataset in section V. Section VI concludes and point out some of the directions for future work.

II. Related Work

Our work on assisting user in identifying the intended audience is an amalgamation of many research interests. Setting visibility to profile items, community extraction, tie-strength determination and Social Identity Management (SIdM) are the main, orthogonal, research interests.

Due to the lack of clear visualizations' availability in social networks, that map to the mental model of users, privacy wizards [4], [17] have been proposed. These wizards assist user in setting visibility to profile items, but, there is an equal need to assist user in determining the right target audience for a post. On the other hand, [15] consider profile items in determining the privacy score. Even though privacy scoring helps user in his awareness of the risks involved in sharing information with other user, it does not hold his hands in defining a policy for sharing.

Community extraction and clustering have been proposed as ways to create groups for a user. Community extraction using network graph has been extensively studied by [5], [19], [20] and has been particularly tested in social networks community detection in [11]. Jones et. al [11] try to answer the common criterias considered by users while creating groups through a survey of Facebook users. Clustering algorithm SCAN [30] was used to group users and test how it fared when compared to user created groups. The results show that the manually created groups overlap with automatically created groups using the clustering algorithm by 44.83%, which is very low and impractical for real-life applications.

Gilbert and Karahalios's [6] studied tie-strength as being dyadic in nature and classified strengths in social networks as either strong or weak. Statistical modelling considering linear combination of predictive variables, 67 of them, is used in determining whether a tie is strong or weak. This supervised method considers tie strength as a binary prediction. Xiang et al [29] study tie-strength to be spanning the whole spectrum from weak tie to strong tie. They propose a latent variable model that considers profile features as discriminative and communication as generative in nature, in determining tie-strength.

Social Identity Management (SIdM) and context-aware, social sphere based audience segregation provide a new paradigm in achieving privacy in a socially networked world as well as a way of presenting and maintaining a consistent self-image as appropriate to the audience. User's social sphere could be manually segregated by the user to create different contexts, social spheres or groups of segregated audience. Van den Berg et. al [25] have proposed *Clique* a privacy preserving social network site. Manual audience segregation again rests the task of creating groups on user, which is not desirable. SIdM, as proposed by [22] gives an alternative way of achieving privacy by decoupling the burden of social identity management (SIdM) from social network provider, to achieve contextually segregated audience. SIdM, provides an alternative way of achieving privacy in an ideal setting, but does not answer the burning question of how to enhance privacy in the already popular social networks like Facebook, Google+, Myspace and others.

Regroup [1] is a Facebook application developed to assist user in creating groups on-demand, thereby avoiding embarrassing oversharing. As the user keeps on adding friends to the group being created, active machine learning is employed to learn the shared features and bring up the best matches to the top of the suggestion list. The research question being addressed by Regroup is same as being addressed by this paper. Finding the intended audience can be seen as privacy-aware group creation problem. They propose to use features shared between friends to identify the right set of target audience for a post, whereas we propose to use only those shared features that can define the context of post. Kahanda and Neville [12] in their work on prediction of link strength, use transactional data in finding if a link or tie is strong or weak. They group the obtained attributes into features to perform the classification using supervised learning. They consider only profile and communication characteristics and do not use context in their classification.

TABLE 1
INFORMATION SHARING SCENARIOS ON FACEBOOK

	Post	**Intended audience**	**Facebook items to capture context**	**Probable audience with Tie-Strength model**	**Probable audience with Context model**
Example 2	Post contains information about a musician from Iran with information written in Persian language. The post also contains a Youtube video of the musician's song rendition	Family and selected close friends who can understand Persian	1. Language = Persian 2. Places lived/Hometown = Places in Iran 3. Education institution location/Work Location in Iran	All Facebook friends with high tie-strength	All Facebook friends satisfying context
Example 3	Post is requesting information on a particular product's implementation. Contains confidential details	Selected current colleagues from Company xx with whom the user regularly communicates	1. Work and Education = Company xx	All Facebook friends with high tie-strength	All Facebook friends satisfying context

III. BACKGROUND

A. Need for the proposed model

The central motivation to using social networks as noted by Tufekci [24] is being seen by those we wish to be seen by. In real life, we give out information based on our audience, sometimes withholding information when we are in the company of in-appropriate audience with respect to the information. But, due to the current social network setting, all social sphere's or contexts collapse, flattening out multiple distinct audiences into one singular group of recipients forcing user's to find alternative ways to manage a large and diverse set of connections [26]. Consider a common sharing scenario as in Example 1.

Example 1: Ana would like to share some pictures of her best friend Sara's wedding, with her friends. She would like to restrict it to a) Only close friends that are common to Sara and her b) Among the close friends to those who were invited and attended. The available way in current social network setting is to select people one by one or to create a group, manually adding people into it and use this group to send photos.

Creating group for every such occasion and sharing requirement is not only cumbersome but difficult to manage. Instead, with our model, information can be sent to only those friends who have a high tie-strength (close friends) along with satisfying the condition that they were invited for the wedding, the context.

Since, social networks consider all friendships equal and call them as *friends*, by using tie-strength, *friends* could be differentiated based on the tie-strength they share with the user. But, tie-strength alone cannot differentiate people from different social sphere's and hence basing information dispersal only on tie-strength will lead to unintended people included as target audience.

In Example 1, Ana would like to distribute photos to her close friends (high tie-strength). But, this alone may not be enough as she wants to send it only to those close friends who attended the wedding (context: Facebook invite as a context and as a source of context information). Hence, context is essential along with tie-strength. Considering sending wedding photos to all those invited by Sara (context: Facebook invite) may not be desirable too as there may be people who are just Ana's acquaintances along with her close friends. Hence, context alone will not be sufficient.

Context of information about to be posted is a rich source of metadata about the actual information itself. Context, here is, a composite attribute. The attributes that define a context are varied. Attributes of context can be content of the post, event, geographic location of the post, geographic location of the content, language, relationship, datetime. By considering the relevant context attributes to each post and finding the friends who have a high context attribute similarity, can be a real distinguisher of intended audience for a post. Social circles can be identified by these context defining attributes. Hence, we use *social circles* and *context* inter-changeably in this paper. The requirement here is not to suggest all the friends who need to be added, but, to highlight those from the selected recipients list who do not match the rest in tie-strength and context.

Table 1 gives two scenarios extracted from the Facebook dataset used in the experiments, explained later in section V. Table contains information about two posts. It is notable that in both the examples, and many such real life sharing scenarios, only tie-strength or only context based information dissemination does not suffice. This requisites users to manually select users to whom they would like to share information. Evidently, to answer such sharing needs, there is a need for the Proposed model which makes use of both tie-strength and context. We omit the explanation of examples 2 and 3 in view of space.

B. Need for Privacy as a service

Understanding and changing privacy settings on social networking site places significant cognitive burden on users, which pushes them to accept the default settings available. With the use of multiple social networking sites, users are forced to set privacy in each site separately. Privacy settings are manually selected for individual user or groups. With differing privacy options across multiple sites with multiple ways of setting privacy, user is laden with the responsibility of setting privacy uniformly across applications. Applications (Apps) development and consumption among social network users is growing. This brings to the fore, problem of controlling privacy across all apps, by the social networks and users alike. Privacy as a service has advantages over privacy incorporated individually into each social network.

IV. PROPOSED MODEL

The proposed Privacy as a service employs a supervised learning model using labelled examples of intended audience. Different from previous work, we propose to use both context

of information and tie-strength between user and his friends (for the rest of this paper, *user* means the social network user who wants to publish a post and *friends* are the user's friends in that social network) as features in learning, for each user-context pair. Friends are classified into intended audience based on the learnt model.

A. Preliminaries

Tie-strength features: The central concept of tie-strength is homophily [18]. Principle of homophily hypothesizes that people form ties with those people who have similar interests and characteristics to theirs, with a stronger tie being formed indicating a higher similarity [7]. We propose to find similarity in profile elements of a social network user along with utilising the communication characteristics. Profile similarity and communication characteristics have been shown to be good indicators of tie-strength [6], [29] and have been used to derive tie-strength value. We propose to use profile similarity and communication characteristics as features in learning. Our aim is to learn a predictive model of tie-strength using labeled training data with predictions of strong tie or weak tie as the expected outcome.

TABLE 2
LIST OF FEATURES

Features	Profile items
General Profile Similarity	Work And Education
	Work And Education Location
	Places Lived
	Countries Lived
	Hometown
	Languages
	Religious Views
	Political Views
	Family
Group Profile Similarity	Events
	Groups
	Mutual Friends
	Likes
Written on wall - 1 year	Written on wall - one year
	Other way round - one year
Tagging - 1 year	Tagged together in a post/photo - one year
Written on wall - Till date	Written on wall - Till date
	Other way round - Till date
Tagging - Till date	Tagged together in a post/photo - Till date

Profile similarity and communication have been divided into features as shown in Table 1. Friends are scored based on what percentage of their profile matches the user. Single valued social network items, like, religious and political views, family are scored as boolean match (1/0), whereas multi-valued items, like, mutual friends, are calculated as percentage of match. Profile items are grouped together meaningfully to capture the common circumstances of user and his friends. The values of each feature is calculated as the summation of the individual items.

General profile similarity gives the similarities shared in profile items of a user and his friend and *Group profile similarity* scores the mutual likes and groups they share along with common events and friends. Wall posts captures posts on friend's wall or post on user's wall by friend. Stronger ties typically use multiple, redundant channels to communicate, as suggested by media multiplexity [9]. Therefore, offline interaction would lead to stronger ties online. Wall Posts and Tagging, together account for the Communication strength feature. The recency of communication has been accounted for by dividing the communication into *Last year communication* and *Till date communication* features used in learning.

Context features: Context similarity is measured based on how many context defining attributes are common between friend's context attributes and the post's context attributes. Intended audience determination service requires user to input information about to be posted (*Post*) and choose context_type-content_type pairs from among the choices provided using the pre-learnt model. User would then choose attributes, from among the available attributes list. This attribute list is the items that can be extracted from social network, in our study - from Facebook, to define a Context. It is notable that the model will function in the absence of any inputs from user, by using only the tie-strength features, albeit being less functional.

Context is made up of composite attribute set. A standard set of pre-learnt attributes or user provided attribute information can be used to denote the context of the information about to be posted. In this study, the users chose to provide the attribute information from among the profile items. These items were scored as 1 if the user and his friends values matched, 0 otherwise. The attribute values, summed together make up the *Specific context similarity*, another feature in learning.

Table 3 gives examples of context_type, content_type, attributes and corresponding profile information or communication information from social network that could be used to measure the similarity.

B. Framework

The framework to classify users into intended audience and unintended audience for each post consists of three main parts:

User input: User inputs the post, for which the intended audience are to be determined. The service expects user to select the context_type-content_type and provide context defining attributes. The service could assist user by providing example scenarios and choices to choose, from the pre-learnt model. Only input compulsory is *Post* and all other inputs are optional.

Feature extraction: For each user, his friends are extracted and their feature scores calcualted. The scores are calculated by matching all the information of user and his friend for each item in social network, with score being, the percentage of matching information. As each additional friend is added, features are extracted and feature scores stored. Feature extraction is triggered with each additional post from the user or each addition of friend or both, as set by the user. Feature extraction could also be triggered by changing of items' values (eg., adding a new work company name), although such changes are not done very often.

Learning and classification: Positive samples are derived from sent friends list and those who have not received the post form the negative samples for the context. Classification techniques are used to learn the classification for the first time,

TABLE 3
SAMPLE LIST OF ATTRIBUTES FROM FACEBOOK

Context Type	Content Type	Attributes	Item in SN
Political, Patriotic	Generic	Geographic Location of the content	Places Lived, Tagged locations of the posts
		Political orientation	Political Views
		Language	Languages
Cultural, Religious	Sensitive	Geographic Location of the content	Places Lived
		Language	Languages
		Religion	Religious Views
Workplace	Sensitive	Workplace name	Work and Education
		Work and Education Location	Derived from work and Education
Photos	Sensitive	High number of mutual friends	Mutual friends
		Event corresponding to photos	Event Invite
		Tagged together often in posts/photos	Tagged Photos and posts
		Communication	Number of mutual wall posts in last one year
			Number of mutual wall posts - till date
Sensitive Information	Sensitive	Communication	Number of mutual wall posts in last one year
			Number of mutual wall posts - till date
		Previously received content	Previous post in the same context
Thoughts	Self-expression	Language	Languages
		Communication	Number of mutual wall posts in last one year
			Number of mutual wall posts - till date

from user posts. Subsequently, it could be triggered everytime the user posts a new post or as and when triggered by the user. User could choose to use only tie-strength feature set (by providing only post as user input) or all features for learning and classification.

User starts by choosing friends from a set of pre-defined groups or selects everyone of his friends as the intended audience for the post. Service is invoked before posting this new information. The learnt model is then utilised to suggest friends who do not match the learnt model and need to be reviewed as possible unintended audience, by the user, before posting.

C. Formal definition

Let $O = \{O_1, O_2, O_3, ...O_j\}$ be a set of friends for the user U_i. Let $I = \{i_1, i_2, i_3, ...i_n\}$ be the information (Post) that has originated from User U_i and has destination as friends $O^{'}$, such that $O^{'} \subseteq O$. Here, $O^{'}$ gives the right target audience for a piece of information i_n. Each information i_n is part of a context C_t, such that $C_t \in \{C_1, C_2, ...C_t\}$. Let $T_{ij_{C_t}}$ be the tie-strength between U_i and O_j, in context C_t.

The goal is to learn a predictive model of $T_{ij_{C_t}}$ using labeled training data. We consider our work to be the dyadic task of predicting whether or not tie-strength $T_{ij_{C_t}}$ is strong to necessitate thrusting friend O_j into set $O^{'}$.

The features used in the supervised learning are General profile similarity GP_{sim}, Group profile similarity GrP_{sim}, Communication similarity yearly $Comm_{sim_{yearly}}$, Communication similarity tilldate $Comm_{sim_{tilldate}}$, and Specific context similarity $S_{C_{tsim}}$.

D. Service Implementation

This section briefly describes the implementation of Privacy service. The architecture diagram is as shown in Figure 1. Privacy as a service accepts user input and provides intended audience recommendations based on a model learnt specific to that user. Privacy service can work with multiple social networks, thereby assisting user in maintaining consistent privacy across all social networks.

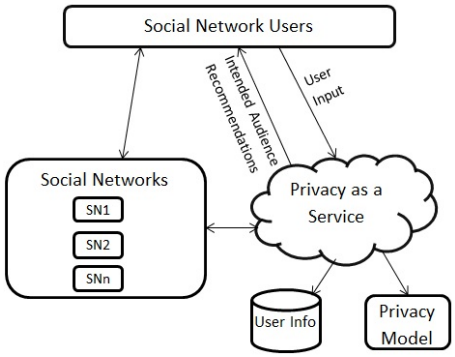

Fig. 1. Service Architecture

Control flow diagram of the implementation of Privacy service in social networks is shown in Figure 2. User interaction with the service is kept simple and to a minimal as seen from the Control flow diagram. This is so as to reduce cognitive burden on the user. User is also assisted in choosing the attributes with recommendations for context_type-content_type selected. By giving an option to select *ALL* for probable friends to whom the user might want to send the post, the service takes control in choosing the intended audience. It is notable that, user will choose the final intended audience list and Privacy service only acts as a recommender basing its recommendations on the learned model, specific to each user.

The critical component of the service is learning from user data. The accuracy of predictions from learned model depends on the nature of data and importantly, on the classification techniques involved. With the use of both basic and advanced techniques we wanted to confirm the effectiveness of the features selected for classification. We first introduce two basic techniques (Naive Bayes, k-NN) that are computationally inexpensive. Social networks data is often of high variance with missing data and incomplete data, a common occurance. We introduce two techniques (LMNN, GB-LMNN) that are,

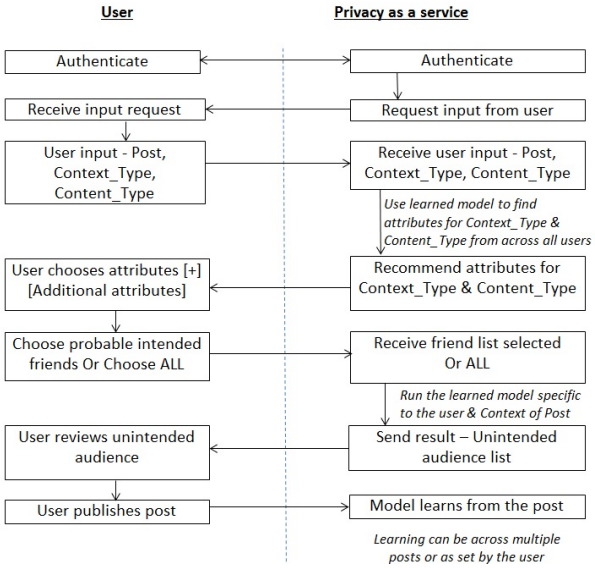

Fig. 2. Control Flow diagram of Privacy service

although computationally expensive than the basic techniques, tolerant towards variance, imbalance and missing data. We compare the effectiveness of each method against the proposed model in experiments section.

1) Naive Bayes: Naive Bayes classification [14] is a probabilistic classifier with assumption of independence between features. The classifier combines the Naive Bayes probability model with a decision rule to pick the most probable outcome, that is known as maximum a posteriori or MAP decision rule. Applying, Naive Bayes classifier, is thus given as in (Equation [1]) -

$$argmax_{O'}\ p(O') \prod_{j=1}^{n} p(F_j|O') \tag{1}$$

where F_j = $\{GP_{sim},\ GrP_{sim},\ Comm_{sim},\ S_{C_{t_{sim}}}\}$ and $p(F_j|O^{'})$ is the likelihood of a friend with feature values from set F_j being a member of $O^{'}$, the intended audience class.

2) k-Nearest Neighbors: k-Nearest Neighbors [2] or k-NN is a non-parametric technique which is used for classification. In this technique, k closest neighbours to each input is found and the input is classified based on the majority vote of its nearest neighbors. In this paper, Mahalonobis metric is used to calculate the distance of sample which is defined as

$$d(x,y) = \sqrt{(x-y)^T M (x-y)} \tag{2}$$

where M is the covariance matrix of vectors x and y.

3) Large Margin Nearest Neighbour (LMNN): The LMNN objective is twofold [28]: decreasing the distance of each data point from its target neighbors by pulling the target neighbors closer to data point (Equation [3]). Target neighbors of each data point are the closest instances to it with the same class label as the data point.

$$\xi_{pull}(L) = \sum_{j \rightsquigarrow i} \parallel L(X_i - X_j) \parallel^2 \tag{3}$$

The second goal is, increasing the distance of each data point and its imposters by pushing the imposters further apart. The imposters are instances with different class labels where their distances are less than target neighbours of the data point. The pushing function is defined as follows (Equation [4]):

$$\begin{aligned}\xi_{push}(L) = \sum_{i,j \rightsquigarrow i} \sum_{l} (1-y_{il})[1+ \parallel L(X_i - X_j) \parallel^2 \\ - \parallel L(X_i - X_l) \parallel^2]_+\end{aligned} \tag{4}$$

These two functions are combined to introduce loss function of LMNN (Equation [5]).

$$\xi(L) = (1-\mu)\xi_{pull}(L) + \mu\xi_{push}(L) \tag{5}$$

Where $\mu \in [0,1]$ is a weighting parameter to balance the objectives.

4) Gradient Boosting Large Margin Nearest Neighbour (GB-LMNN): Since LMNN is unable to find non-linear similarities between data points, GB-LMNN was proposed [13], in which LMNN is generalized to a non-linear transformation ϕ, where combination of gradient boosted regression trees is applied to find a right form of ϕ (Equation [6]).

$$\phi = \phi_0 + \alpha \sum_{t=1}^{T} (h_t) \tag{6}$$

Where h_t is a regression tree weighted by α and ϕ_0. Taylor approximation ζ is applied to find the optimal tree h_t(Equation [7]).

$$\begin{aligned} h_t = argmin_{h \in T^p} \sum_{i=1}^{n} (g_t(X_i) - h_t(X_i))^2 \\ \text{where } g_t(X_i) = \frac{\partial \zeta(\phi_{t-1}))}{\partial \phi_{t-1}(X_i)} \end{aligned} \tag{7}$$

V. Experiments

This section evaluates the effectiveness of the proposed model in finding the appropriate target audience for information to be posted in Facebook. The proposed service has been tested by using the four classification techniques described in the previous section. These classification techniques are used to classify user's friends (denoted by O) to either being the right target audience (denoted by $O^{'}$) or as unintended audience (denoted by $O - O^{'}$). We collected the profile items and communication data from selected friends of the user making sure both classes $O^{'}$ and $O - O^{'}$ were represented.

Proposed model has been tested with one of the most popular social network, Facebook. Model would work on other popular social networks too, as they contan similar user profile and communication information. LinkedIn provides features such as school, company, geographic region, industry, job area, common groups and connections that could be used to find the profile similarity with establishing a connection, writing a recommendation, profile viewing useful for communication similarity. Google+ provides profile information in the form of education, occupation and employment information, places lived, skills, common events and communities for profile similarity and messages, tagging can be considered for communication similarity.

A. Evaluation

For evaluation, we collected profile similarity, communication and specific profile similarities of 230 pairs of Facebook users, with each pair consisting a user and his friend. 230 users represent 6 different nationalities. On an average, users have been friends since 23 months. Posts were collected for a duration of 4 months starting from October 2013 till January 2014. A total of 6 contexts were identified from a set of 106 posts. The results of 6 posts, each representing a unique context and sharing pattern have been discussed in the results section.

The similarity values of General and Group profile similarity, Last year and Till date communication similarity values are obtained as continuous data. The contexts of post, varied from being too sensitive content_type to general information. The posts used in experimental evaluation had on an average 3 context defining attributes that could be extracted. We held out 20% of records as test and used 80% to learn the model. Accuracy values are obtained by averaging over 100 runs. Example context defining attributes collected during the experiments have been listed in the Table 4.

TABLE 4
EXAMPLE CONTEXT DEFINING ATTRIBUTES EXTRACTED DURING EXPERIMENTS

Religious views
Language of post
Event of photo
Family
Places lived
Location of the post
Educational or Work institution
Educational or Work location
Tagged together
Received item belonging to context, previously

Table 5 gives a snippet of the records with values for various attributes. The records indicate the importance of selected features in identifying the right target audience. In particular, classification 'Yes' indicates, right target audience. Record 1 has high Group profile similarity, though it lacks communication. This is a classic case of a friend being just *observer* in social network communication with the user. Records 2, 3, and 5 are intended audience, owing to them having a high communication similarity value. All 'Yes' records also have Specific context similarity value > 0 (tie-strength + context). All 'No' classifications, have Specific context similarity value as 0 (no context similarity) other than record 11 . Record 11 is very low in profile similarity and communication feature values and hence classified 'No', even though it has high Specific context similarity (low tie-strength, high context similarity).

B. Results and discussion

Using Naive Bayes, k-NN, LMNN, GB-LMNN, user's friends were classified as belonging to intended audience or unintended audience. The results are as shown in Table 6. The table shows the comparison of accuracy of the proposed model as compared with classification on only Tie-strength and only Context.

Key observations:

TABLE 6
CLASSIFICATION ACCURACY IN PERCENTAGE

		Proposed method	**Tie-strength**	**Context**
Post 1	Bayes	81.8	81	50
	k-NN	75.1	73.2	41
	LMNN	78.9	74	41
	GB-LMNN	81.1	72.7	41
Post 2	Bayes	76.4	71.9	75.4
	k-NN	74.2	71.4	54.5
	LMNN	75.6	74.8	54.5
	GB-LMNN	76.1	77.6	54.5
Post 3	Bayes	83.7	83.2	78.7
	k-NN	77.7	76.3	78.7
	LMNN	81.3	78.9	78.7
	GB-LMNN	82.5	81.2	78.7
Post 4	Bayes	61.9	65.2	85.7
	k-NN	90.48	88.1	85.7
	LMNN	90.48	85.7	85.7
	GB-LMNN	95.24	87.1	85.7
Post 5	Bayes	66.6	64.2	74.4
	k-NN	80.7	81.3	73.9
	LMNN	79.3	79.5	73.9
	GB-LMNN	77.4	78.3	73.9
Post 6	Bayes	78.2	63.5	96
	k-NN	84.1	80.3	96
	LMNN	92.56	79.7	96
	GB-LMNN	93.84	78.3	96

- Regardless of the chosen classification method, the proposed model works better than classification based on only tie-strength features or only context features.
- LMNN and GB-LMNN give better result due to their tolerance towards data variance.
- GB-LMNN performs the best.

Post 1,2,4,5: Accuracy supports the proposed method. In all cases, the proposed method performs better than classification based on tie-strength or context alone.

Post 3: Jones et al. [11] work identifies group creation, and further postings to the group, being influenced by tie-strength. In post 3, classification based on the proposed method performs no better than classification based on tie-strength alone. Sending a post to all best friends, is a notable example.

Post 6: In this post, we can observe that profile similarity or communication is not an influencing factor in determining the intended audience. GB-LMNN accuracy (93.84%) is comparable to classification based on context alone (96%). Work on group creation in social networks [1], [11] have shown that social circles is a major factor in the creation of groups and in some-cases, social circle alone is the defining criteria. There are also situations where no suitable context defining attributes can be mapped to social network items. In Post 6, the situation was later; we could not identify a suitable attribute able to identify the context of information in post. Hence, we made use of *Received item belonging to context, previously* as an attribute. The results clearly show this is a very sensitive attribute in identifying the classes correctly. It is notable that *Received item belonging to context, previously* can be used, when there is a previous occurance that can be fed for learning.

TABLE 5
RECORDS SNIPPET

	Recd 1	Recd 2	Recd 3	Recd 4	Recd 5	Recd 6	Recd 7	Recd 8	Recd 9	Recd 10	Recd 11
General Profile Similarity	5.25	3.75	1.75	0.50	3.00	1.00	0.50	0.50	0.50	0.50	3.75
Group Profile Similarity*100	131.45	57.14	9.61	1.05	8.10	1.05	11.12	17.53	8.98	1.05	10.74
Yearly Communication	0	2	4	2	2	2	0	0	0	0	0
Tilldate Communication	0	14	10	5	9	5	2	2	2	1	0
Specific Context Similarity	2	2	2	0	1	0	0	1	0	0	2
Classification	Yes	Yes	Yes	No	Yes	No	No	Yes	No	No	No

VI. CONCLUSION AND FUTURE WORK

We have proposed Privacy as a service model to assist user in choosing the intended audience for a post in social networks. The service uses tie-strength and context similarity as features in supervised learning. The proposed service, solicits input from user in the form of actual information to be posted, attributes, optionally accepting additional new context defining attributes. Comprehensive experiments prove that our model provides acceptable accuracy in most cases and can work even in the absence of context attributes altogether. The proposed privacy service can assist in identifying friends who do not belong to the intended audience. Our ongoing work includes addressing the problem of blind spots [27] in social network analysis and deriving a learning algorithm for friend addition or post updates from new contexts.

REFERENCES

[1] S. Amershi, J. Fogarty, and D. Weld. Regroup: Interactive machine learning for on-demand group creation in social networks. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 21–30, 2012.

[2] T. Cover and P. Hart. Nearest neighbor pattern classification. *Information Theory, IEEE Transactions on*, 13(1):21–27, 1967.

[3] 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, 2011.

[4] L. Fang and K. LeFevre. Privacy wizards for social networking sites. In *Proceedings of the 19th international conference on World wide web*, pages 351–360, 2010.

[5] S. Fortunato. Community detection in graphs. *Physics Reports*, 486(3):75–174, 2010.

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

[7] M. Granovetter. The strength of weak ties: A network theory revisited. *Sociological theory*, 1(1):201–233, 1983.

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

[9] C. Haythornthwaite. Social networks and internet connectivity effects. *Information, Community & Society*, 8(2):125–147, 2005.

[10] W. Itani, A. Kayssi, and A. Chehab. Privacy as a service: Privacy-aware data storage and processing in cloud computing architectures. In *Dependable, Autonomic and Secure Computing, 2009. DASC'09. Eighth IEEE International Conference on*, pages 711–716, 2009.

[11] 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, 2010.

[12] I. Kahanda and J. Neville. Using transactional information to predict link strength in online social networks. In *ICWSM*, 2009.

[13] D. Kedem, S. Tyree, K. Q. Weinberger, F. Sha, and G. R. Lanckriet. Non-linear metric learning. In *NIPS*, pages 2582–2590, 2012.

[14] P. Langley, W. Iba, and K. Thompson. An analysis of bayesian classifiers. In *AAAI*, volume 90, pages 223–228, 1992.

[15] 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 (TKDD)*, 5(1):6, 2010.

[16] E. M. Maximilien, T. Grandison, T. Sun, D. Richardson, S. Guo, and K. Liu. Privacy-as-a-service: Models, algorithms, and results on the facebook platform. In *Proceedings of Web*, volume 2, 2009.

[17] A. Mazzia, K. LeFevre, and E. Adar. The pviz comprehension tool for social network privacy settings. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, page 13, 2012.

[18] M. McPherson, L. Smith-Lovin, and J. M. Cook. Birds of a feather: Homophily in social networks. *Annual review of sociology*, pages 415–444, 2001.

[19] M. E. Newman and M. Girvan. Finding and evaluating community structure in networks. *Physical review E*, 69(2):026113, 2004.

[20] A. Noack. Modularity clustering is force-directed layout. *Physical Review E*, 79(2):026102, 2009.

[21] J. S. Olson, J. Grudin, and E. Horvitz. A study of preferences for sharing and privacy. In *CHI'05 extended abstracts on Human factors in computing systems*, pages 1985–1988, 2005.

[22] M. Riesner and G. Pernul. Provider-independent online social identity management–enhancing privacy consistently across multiple social networking sites. In *System Science (HICSS), 2012 45th Hawaii International Conference on*, pages 800–809, 2012.

[23] K. Strater and H. R. Lipford. Strategies and struggles with privacy in an online social networking community. In *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction-Volume 1*, pages 111–119, 2008.

[24] Z. Tufekci. Can you see me now? audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, 28(1):20–36, 2008.

[25] B. van den Berg and R. Leenes. Audience segregation in social network sites. In *Social Computing (SocialCom), 2010 IEEE Second International Conference on*, pages 1111–1116, 2010.

[26] J. Vitak. The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting & Electronic Media*, 56(4):451–470, 2012.

[27] D. Wang, X. Liu, and X. Li. Blind spots: Unveiling users' true willingness in online social networks. In *Global Communications Conference (GLOBECOM), 2012 IEEE*, pages 2066–2071, 2012.

[28] K. Q. Weinberger and L. K. Saul. Distance metric learning for large margin nearest neighbor classification. *The Journal of Machine Learning Research*, 10:207–244, 2009.

[29] 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, 2010.

[30] X. Xu, N. Yuruk, Z. Feng, and T. A. Schweiger. Scan: a structural clustering algorithm for networks. In *Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 824–833, 2007.

[31] A. L. Young and A. Quan-Haase. Information revelation and internet privacy concerns on social network sites: a case study of facebook. In *Proceedings of the fourth international conference on Communities and technologies*, pages 265–274, 2009.

[32] X. Zhao, J. Yuan, G. Li, X. Chen, and Z. Li. Relationship strength estimation for online social networks with the study on facebook. *Neurocomputing*, 95:89–97, 2012.