Adaptive sharing for online social networks: a trade-off between privacy risk and social benefit

Conference or Workshop Item

Adaptive Sharing for Online Social Networks: A Trade-off between Privacy Risk and Social Benefit

Mu Yang, Yijun Yu, Arosha K. Bandara
The Open University, UK

Bashar Nuseibeh
The Open University, UK and Lero, Ireland

***Abstract*—Online social networks such as Facebook allow users to control which friend sees what information, but it can be a laborious process for users to specify every receiver for each piece of information they share. Therefore, users usually group their friends into social circles, and select the most appropriate social circle to share particular information with. However, social circles are not formed for setting privacy policies, and even the most appropriate social circle still cannot adapt to the changes of users' privacy requirements influenced by the changes in context. This problem drives the need for better privacy control which can adaptively filter the members in a selected social circle to satisfy users' requirements while maintaining users' social needs. To enable such adaptive sharing, this paper proposes a utility-based trade-off framework that models users' concerns (i.e. potential privacy risks) and incentives of sharing (i.e. potential social benefits), and quantifies users' requirements as a trade-off between these two types of utilities. By balancing these two metrics, our framework suggests a subset of a selected circle that aims to maximise users' overall utility of sharing. Numerical simulation results compare the outcome of three sharing strategies in randomly changing contexts.**

I. Introduction

Online social networks provide people new opportunities for interaction and socialization. As a result, users' personal information, including profile data, location and activities are increasingly shared with online friends via online social networks, comprising families, friends, coworkers and even strangers. With the dramatically increased number of users and amount of information sharing, the question of whether online social networks provide users good privacy control over their personal information is particularly important.

Online social networks such as Facebook and Google+ allow users to control which friends see what information, but users who are not aware of privacy often share information without considering who should (or should not) access it. Even privacy-aware users sometimes may make wrong decisions because of a lack of skill and information about risks and consequences of sharing [2], [17]. Moreover, specifying every receiver for each piece of information they share can be a laborious precess, especially when they have several hundreds of online friends [13]. Users thus usually share information by choosing the most appropriate social circle from their pre-defined social circles which are grouped according to different types of relationships, e.g., family, classmate, living in the same city, etc. However, social circles are not formed for setting privacy policies, and rather are relatively static groupings of different types of friends [15]. For privacy management, users require dynamic social circles to match each of their sharing intentions, and these social circles must be able to adapt to the changes of users' privacy requirements which are influenced by *contextual* factors [5], [16], such as sensitivity of information, trustworthiness of information receivers, etc. However, these changes are not predictable when forming social circles. Therefore, better privacy control is needed, which can capture these changes at runtime and then adaptively filter the members in users' selected sharing circles each time before sharing their information.

There have been several attempts to solve this adaptive sharing problem [3], [6], [4]. These studies make the assumption that users are privacy-aware and their historical sharing decisions do not cause privacy problems. They proposed schemes that automatically form new social circles to adapt to users' changing context and sharing requirements, by predicting users' decisions based on their historical ones. However, because users may make poor decisions, these schemes may adversely affect users' privacy. A novel approach to determine the *optimal* sharing decision within the selected social circle rather than just predict decisions that are most likely to be chosen remains an open research topic. In particular, it requires an analytical framework to predict, quantify and trade-off the potential privacy risks and social benefit with respect to each of the information receivers in the selected social circle. This is a challenging and fundamental problem. Indeed, if we cannot quantify and trade-off these, we will not be able to determine with whom users should share in the selected social circle, given particular information in a given context. The trade-off between the potential social gains and privacy risks of sharing requires users' own preferences over them, and hence users must be involved and the framework must be able to take into account users' preferences every time they share.

Simplifying social networking scenarios on the basis of two popular privacy threats [8], we assume four possible activities information receivers may undertake regarding the information: re-share, misuse, respond, and do nothing. We will describe the details of our threat model and these activities in §II. Given the threat model and these four activities, we select several contextual factors for the quantification of potential sharing risks and benefits. By using these factors, we illustrate how to build a utility-based trade-off framework that quantifies users' privacy risks and social benefit for sharing their information with each of the members in the selected sharing circle. We then study the trade-offs between these two types of utility under different settings of these factors. Finally the trade-offs enable our solution for adaptive sharing to recommend that users should share information within an optimally selected social circle, adapting to changing contextual factors at runtime. The effectiveness of our adaptive sharing framework is evaluated with a simulation of randomised contextual factors.

II. Motivating Example

A. Sharing activities and social circles

Users have a range of information-sharing activities in various online social networks, such as making their profile information visible, posting their location, photos and any other personal related information, and sending private messages to people whom they are socially connected with, and so on. We generalise these information-sharing activities as *disclosing some information to at least one friend*. We assume that the friend(s) who receive(s) the information has/have a choice of four actions to perform using the information:

Re-share: the information receiver re-shares the information with her own friends.
Misuse: the information receiver uses the information for improper purposes, such as stalking, identity theft, sending spam messages, etc.
Respond: the information receiver leaves comments on the information, or express opinions about it, such as the Like function on Facebook.
Do nothing: the information receiver does not do anything about the information, except for seeing it.

Note that the first three activities are not mutually exclusive, information receivers may do them at the same time.

Users usually group their friends into different *social circles* to manage friends relationship, such as immediate family, university friends, and so on. Conveniently, users pick one or more social circles to share a specific piece of information, instead of selecting friends individually. However, users can still exclude/add friends individually from/to the selected social circles. The final chosen friends to receive the information form a new social circle for this particular information sharing, and we name it *selected social circle*, in which our adaptive sharing approach aims to filter the members.

B. Privacy threats

In this paper, we focus on two types of privacy threats based on a privacy investigation survey [8] on Facebook users.

- **Stranger danger** Social networking users are concerned about the visibility of their information, the survey [8] found almost half of their participants prohibits strangers from viewing their information. However, once the information is received by the selected sharing friends, users lose control over it. Information receivers may re-share the information with their own social circles, making the information more visible [9]. We name the people who are not original in users' selected sharing circle as *unintended recipients*.
- **The insider threat** Facebook reports that the average user has 130 friends [1]. These can be broadly categorised as "immediate family", "school friend", "socialised with", "coworker", "friend have not met", etc. Different groups of friends naturally represent different *trustworthiness* of receiving information [8]. *Untrustworthy friends* have a greater likelihood of misusing the information. Sharing all information with all the friends without filtering them causes privacy risks.

C. A motivating example

To have a concrete example, we consider a user Alice (a) who has two social circles: University Friends and Coworkers as depicted in Fig. 1. To share a particular piece of information, for instance, Alice selects University Friends as the selected sharing circle. Friend Bob (b) and Charlie (c) are thus accessible to the information. This selection seems to satisfy both Alice's social needs and privacy requirements. However, privacy might be violated. For instance, assuming Bob is not trustworthy, he misuses the information trying to stalk Alice. Then he should be avoided if privacy is the sole aspect that Alice cares about. Alice's privacy might also be violated if Bob re-shares the information, strangers h and g will see it. Sharing the information with Charlie in this case is safer, as his social connections are within Alice's social graph. But if the social aspect is considered as well and interacting with Bob brings Alice great social benefit, e.g., getting important comments from him, then he might be still worthy of being chosen as the potential social benefit outweighs privacy risks.

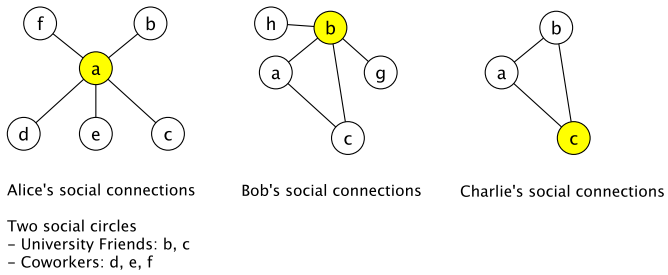


Fig. 1: Social connections of user Alice, Bob and Charlie

The challenge of this example is how to predict the potential privacy risks and social benefit of sharing with each member in the selected social circle, and help Alice trade-off between them to maximise her utility of information-sharing. This assistance is particularly important when users are not able to evaluate privacy risks and social benefit on their own, due to large number of friends in the selected circle, and as well as a lack of information about contextual factors.

III. Model and Metrics

As explained previously, this paper focuses on the analysis of trade-offs between privacy risks and social benefit, which we believe to be key of solving the adaptive sharing problem. In this section, we model users' information-sharing by a utility-based trade-off model and assume users are rational agents trying to maximise their own utility.

A. A trade-off model

We consider a user i who intends to share her personal information $info_i$ with one of her social circles. The selected sharing circle includes n friends, denoted by $N = \{1, \ldots, n\}$ where $n \geq 1$. With regard to each friend $j \in N$, user i typically has two actions *Share* and *Not share*, respectively denoted by $\mathcal{S}$ and $\mathcal{N}$. For simplicity, this paper is only interested in these two actions, and do not consider the situation where users may lie about their information. These two actions are thus independent of i and j. We write $u_{ij}(\mathcal{S})$ and $u_{ij}(\mathcal{N})$ for i's utilities of respective action $\mathcal{S}$ and $\mathcal{N}$ with respect to an

information receiver j. This paper evaluates users' utilities by taking into account two factors: *potential privacy risks* and *potential social benefit* caused by users' strategic actions. These two factors need to be traded off against each other, as privacy risks and social benefit are usually associate with the same sharing decision. Note that typically a user does not suffer any privacy loss if she does not share, but she does not gain any social benefit neither. Therefore, we always have $u_{ij}(\mathcal{N}) = 0$. We define the utility function under action Share as follows.

Definition 1: **(Utility)** For user i, the utility function $u_{ij}(\mathcal{S})$ describes the payoff to her under her action $\mathcal{S}$ with regard to the information receiver j. We assume that the utility function is a linear function over two factor functions $r_{ij}(\mathcal{S})$ and $b_{ij}(\mathcal{S})$ representing the potential privacy risks and social benefit respectively[1]. By using a weight parameter $w_i \in [0, 1]$ to indicate i's privacy preferences, we have

$$u_{ij}(\mathcal{S}) = (1 - w_i)b_{ij}(\mathcal{S}) + w_i r_{ij}(\mathcal{S}).$$

Here the privacy risk function $r_{ij}(\mathcal{S})$ is non-positive as it reflects the loss of sharing. As $u_{ij}(\mathcal{N}) = 0$ always holds, action $\mathcal{S}$ is an optimal action for i if her utility of sharing $u_{ij}(\mathcal{S})$ is greater than zero. Formally:

Proposition 1: An optimal action d^*_{ij} for any $j \in N$ is determined as

$$d^*_{ij} = \arg\max_{s\in\{\mathcal{S},\mathcal{N}\}} u_{ij}(s) = \begin{cases} \mathcal{S} & u_{ij}(\mathcal{S}) > 0, \\ \mathcal{N} & otherwise. \end{cases}$$

Now we define the optimal decision for user i with respect to all j in the selected social circle N.

Definition 2: **(Optimal decision)** $D^*_i = \{d^*_{i1}, \ldots, d^*_{in}\}$ is an optimal decision for user i and the optimal overall utility can be evaluated as

$$\sum_{j\in N} u_{ij}(d^*_{ij}) = \sum_{j\in N, u_{ij}(\mathcal{S})>0} u_{ij}(\mathcal{S}).$$

To determine the optimal action and achieve the optimal utility, we focus on the computation of $u_{ij}(\mathcal{S})$ for the rest of this section.

B. Metrics for predicting privacy risks

The metrics quantifies users' potential privacy risks under the given threat model described in Section II; the greater the absolute value of the quantification, the greater the privacy threat to users. Naturally, privacy risks depend on the sensitivity the user assigns to the information, and the estimated amount of information leakage under the given threat model. The basic assumptions of our quantification of privacy risks are the following.

- The more sensitive information a user shares, the greater her privacy risks.
- Given our assumed threat model (i.e., stranger danger and the insider threat), the more information is predicted to be leaked to unintended recipients and untrustworthy friends, the greater the user's privacy risks.

The following examples illustrate these two assumptions.

Example 1. Assume user i assigns high sensitivity to her work-related information and low sensitivity to the city she lives with regard to her social circle of University Friends. Sharing the work-related information is more risky.

Example 2. Assume user i has two social circles, Family and Friends she never met. Sharing information with the second social circle is more risky, as it results in information accessed by less trustworthy friends.

According to these two assumptions, we define the metrics of privacy risks of user i to be a monotonically increasing function of two parameters: the sensitivity of information and predicted information leakage of sharing. Formally, we have

Definition 3: **(Privacy risks)** For user i, the sensitivity of information $info_i$ is denoted by α_i and depends on i's opinion on $info_i$. The predicted information leakage is denoted by $f_{ij}(\mathcal{S})$ depending on i and also the information receiver j. The potential privacy risks for an information-sharing action with j, denoted by $r_{ij}(\mathcal{S})$, can be any combination of sensitivity and information leakage. For simplicity, the paper uses the product operator to combine them.

$$r_{ij}(\mathcal{S}) = -f_{ij}(\mathcal{S}) \times \alpha_i$$

where $f_{ij}(\mathcal{S})$ and α_i are both normalized to the range of $[0, 1]$. Thus $r_{ij}(\mathcal{S})$ will be normalized to $[-1, 0]$.

The sensitivity level can be obtained by asking for explicit user's feedback, for instance, using a 5-point Likert scale that ranged from "high sensitivity" to "not sensitive at all", with "medium sensitivity" as the neutral option. We then assign the scores to each of the options from the range of $[0, 1]$, particularly 1 for "high sensitivity" and 0 for "not sensitive at all". The sensitivity level can also be obtained by analysing users' historical sharing decisions [11]. We leave the question of which approach should be chosen for future work. We now describe the computation of information leakage below.

We measure users' predicted information leakage by adopting the information-theoretic framework [12] which is widely used to measure the amount of information leakage in secure systems. In particular, we use Shannon's definition of entropy to quantify the predicted information leakage caused by users' sharing behaviours: how much knowledge about the sharing information $info_i$ are learned by unintended recipients and untrustworthy friends. Our proposed measurement model compares the information obtained by unintended recipients and untrustworthy friends after the selected friends receiving the information. Before the selected friends receiving the information, unintended recipients and untrustworthy friends have no idea about it if they do not have any auxiliary information. However, after receiving it, some amount of the information may be leaked to them and then their uncertainty about the information decreases. Naturally, if the information leakage is normalised to the range of $[0, 1]$, then it is one if unintended recipients and untrustworthy friends are sure about the information, representing the information is completely leaked; and zero if they still know nothing about it.

[1] In order to make these two factor functions $r_{ij}(\mathcal{S})$ and $b_{ij}(\mathcal{S})$ comparable, we normalise them to the same range between zero and one. There are other ways of comparing factors which cannot be directly compared, e.g., [10]. This paper does not focus on selecting the best approach to do the comparisons.

Let V_i denote the set containing all possible values that $info_i$ may indicate. The number of elements in V_i is denoted by k where $k \geq 1$. For example, if $info_i$ is a photo and indicates i's gender, then V_i is $\{female, male\}$ and k is equal to 2. Let X denote the discrete random variable with probability mass function $Pr(X = x)$, where x represents each possible value that X may take. Here x corresponds to an element in V_i. The probability $Pr(X = x)$ reflects the knowledge that unintended recipients and untrustworthy friends have about $info_i$. Assuming unintended recipients and untrustworthy friends do not have any auxiliary information, they are able to guess i's gender correctly with probability 0.5 without seeing the photo.

We then denote by $H(X)$ the entropy of a specific social networking application for protecting i's private information $info_i$. It represents the uncertainty of unintended recipients and untrustworthy friends on $info_i$. For each value X might take, unintended recipients and untrustworthy friends assign a probability $Pr(X = x)$. According to [12], $H(X)$ can be evaluated as

$$H(X) = \sum_{x \in V_i} Pr(X = x) \log \frac{1}{Pr(X = x)} .$$

Now we apply the measurement to our information-sharing scenario, we have

Lemma 1: If unintended recipients and untrustworthy friends have no auxiliary information about $info_i$, then

$$H(X) = \log k .$$

Proof: As unintended recipients and untrustworthy friends have no information on $info_i$ before i shares it, the probability $Pr(X = x)$ for each x in V_i is uniformly distributed, which is $1/k$. $H(X)$ can be evaluated as

$$\begin{aligned} H(X) &= k \times \frac{1}{k} \times \log \frac{1}{1/k} \\ &= \log k . \end{aligned}$$

■

Let Y_j be the event that i shares her information $info_i$ with j, and $H(X \mid Y_j)$ be the entropy of the social networking application for protecting $info_i$ given event Y_j. By applying Bayes' Theorem, we have

$$H(X \mid Y_j) = \sum_{x \in V_i} Pr(X = x \mid Y_j) \log \frac{1}{Pr(X = x \mid Y_j)} . \quad (1)$$

Now we compute $H(X \mid Y_j)$ by considering the two types of threats caused by the sharing action. For the stranger danger threat, the probability that each information receiver j re-shares a specific piece of information determines the predicted information leakage. Naturally, the higher the *re-sharing probability*, the greater the information leakage to the unintended recipients. For the insider threat, the information is completed leaked if at least one information receiver misuses it. However, before sharing the information, user i does not know whether each of information receivers, say j will misuse it or not. But she has knowledge on j that how trustworthy j is, based on her previous interactions with j. Therefore, if j is given a high *trust level* by i, then there is less information leaked to untrustworthy friends. We define these two parameters as follows.

Definition 4: **(Re-sharing probability)** The probability that an information receiver j, $j \in N$ re-shares the information $info_i$ with her own social connections is denoted by p_{ij}.

The value of p_{ij} can be easily derived by monitoring the ratio of the number of times that j re-shares over the number of times that j receives information from i in a specific social networking application.

Definition 5: **(Trust level)** The trust level of an information receiver j, $j \in N$, in user i's points of view, is denoted by t_{ij} and $t_{ij} \in [0, 1]$, where $t_{ij} = 1$ represents j is fully trusted by i and $t_{ij} = 0$ represents j is not trustworthy at all.

The value of t_{ij} can be obtained by asking for user i's trust opinion on j, or deriving from the group type that j belongs to. For instance, j will have a high trust level if he belongs to i's immediate family social circle. It is also possible to obtain the value by deploying some reputation schemes in social networks.

Based on these two parameters, we compute $H(X \mid Y_j)$ as follows.

Lemma 2: If unintended recipients and untrustworthy friends have no auxiliary information about $info_i$, then

$$\begin{aligned} H(X \mid Y_j) &= \sum_{x \in V_i} Pr(X = x \mid Y_j) \log \frac{1}{Pr(X = x \mid Y_j)} \\ &= \frac{k - (k-1)t_{ij}(1 - p_{ij})}{k} \log \frac{k}{k - (k-1)t_{ij}(1 - p_{ij})} \\ &+ \frac{(k-1)t_{ij}(1 - p_{ij})}{k} \log \frac{k}{t_{ij}(1 - p_{ij})} . \end{aligned}$$

For the extreme cases when $p_{ij} = 1$ or $t_{ij} = 0$, we assume $H(X \mid Y_j)$ is equal to zero.

Proof: Detailed in [18]. ■

The amount of information that unintended recipients and untrustworthy friends learn from the sharing event can be expressed as $H(X) - H(X \mid Y_j)$. In order to normalise the value, we divide it by $H(X)$. We then obtain the normalised information leakage of sharing as follows.

Proposition 2: The information leakage of user i for sharing her personal information $info_i$ to j is evaluated as

$$f_{ij}(\mathcal{S}) = 1 - \frac{H(X \mid Y_j)}{H(X)}$$

where $H(X \mid Y_j)$ and $H(X)$ are computed in Lemma 1 and 2.

For the extreme case with $k = 1$, we assume $f_{ij}(\mathcal{S})$ is equal to zero in that unintended recipients and untrustworthy friends certainly know $info_i$ irrespective of whether i shares it with j or not. This equation quantifies the information that sharing behaviour leaks, in particular, $f_{ij}(\mathcal{S}) = 1$ means unintended recipients and untrustworthy friends know the information completely; and $f_{ij}(\mathcal{S}) = 0$ means sharing behaviour does not leak any information.

Note that since the measurement of information leakage is based on particular threat models (e.g., stranger danger and the insider threat in this paper), the result is not applicable to all possible threat models. But our measuring model is flexible and able to be applied under different threat models.

C. Metrics for predicting social benefit

In the previous section we developed an information-theoretic model that quantifies users' potential privacy risks in terms of the sharing behaviours. In this section we focus on users' social benefit $b_{ij}(\mathcal{S})$ and measure how much user i is predicted to gain by sharing $info_i$ with j. In this paper, the social gains are evaluated by considering the following two aspects.

- User i gains social benefit if her information is seen by information receiver j and j belongs to the selected sharing circle. We denote this benefit as $\Phi_{ij}^{(1)}(\mathcal{S})$.
- Interactions between i and j. As described in the respond activity in §II, due to the sharing, user i has opportunities to interact with j. In particular, j may comment on i's sharing, or show her opinions (e.g., Like), or any kind of responses to it. They may then have further interactions regarding j's responses. This type of social benefit is denoted by $\Phi_{ij}^{(2)}(\mathcal{S})$.

In order to capture the essence of these two aspects, we first define a general function of social benefit as a combination of all types of benefit.

Definition 6: **(Social benefit)** For user i, the social benefit $b_{ij}(\mathcal{S})$ describes the social payoff to her under her strategies $\mathcal{S}$ in terms of information receiver j. We assume that the utility function of social benefit takes the form of a linear combination of functions $\Phi_{ij}^{(\beta)}$, each accounting for a type β of social benefit, relevant to the specific application. That is, using a weight parameter $v_{i\beta} \geq 0$ to indicate the (relative) weight that user i attributes to type β, then $\sum_\beta v_{i\beta} = 1$ and

$$b_{ij}(\mathcal{S}) = \sum_\beta v_{i\beta} \cdot \Phi_{ij}^{(\beta)}.$$

Given i's preferences denoted by $v_i \in [0, 1]$ and $1 - v_i$ respectively over these two types of social benefits in this paper, we define the function of social benefit as follows.

Lemma 3:

$$b_{ij}(\mathcal{S}) = v_i \Phi_{ij}^{(1)}(\mathcal{S}) + (1 - v_i)\Phi_{ij}^{(2)}(\mathcal{S})$$

This paper only considers these two types of social benefit, but our measurement framework is flexible and able to add other types of benefit for specific applications. In order to normalize both $\Phi_{ij}^{(1)}(\mathcal{S})$ and $\Phi_{ij}^{(2)}(\mathcal{S})$ to $[0, 1]$, we define $\Phi_{ij}^{(1)}(\mathcal{S}) = 1$ as i's seen benefit is fully satisfied. Next we evaluate the interaction benefit $\Phi_{ij}^{(2)}(\mathcal{S})$.

Let m_{ij} denote the ratio of the number of interactions (e.g., comment, like, etc.) between i and j over the number of times that j receives information from i. It represents the average number of interactions for a single sharing event. The value of m_{ij} can be easily obtained by monitoring i's historical sharing behaviours and interactions with friends. We use the ratio m_{ij} to estimate the i and j's interactions for a new sharing event. We divide it by the maximum interaction ratio for different j due to the normalisation, the interaction benefit $\Phi_{ij}^{(2)}(\mathcal{S})$ can be evaluated as follows.

Lemma 4:

$$\Phi_{ij}^{(2)}(\mathcal{S}) = \frac{m_{ij}}{\max\limits_{j \in N} m_{ij}}.$$

Now we have the social benefit of i under strategy $\mathcal{S}$ evaluated as follows.

Proposition 3:

$$b_{ij}(\mathcal{S}) = v_i + (1 - v_i)\frac{m_{ij}}{\max\limits_{j \in N} m_{ij}}.$$

As presented in Proposition 3, when user i only considers the seen benefit, i.e., $v_i = 1$, the social benefit $b_{ij}(\mathcal{S})$ becomes independent with j and is always one under strategy $\mathcal{S}$. This illustrates the situation where a user uses social networks for disseminating information and does not care about the responses received from the information receivers. Her social requirement is fully satisfied as long as the selected information receiver j receives it, and her social benefit increases as the number of receivers (i.e., the size of N) increases.

D. The trade-offs and decision making

In this section, we investigate how to trade-off privacy risks against social benefit in order to enable user i to make an optimal decision.

We substitute the computations of privacy risks and social benefit from Proposition 2 and 3 in our utility definition (see Definition 1), and then evaluate whether $u_{ij}(\mathcal{S})$ for each $j \in N$ is positive in order to determine the optimal action d_{ij}^* (i.e., $\mathcal{S}$ or $\mathcal{N}$). Our utility function is rewritten as

$$u_{ij}(\mathcal{S}) = (1 - w_i)\left(v_i + (1 - v_i)\frac{m_{ij}}{\max\limits_{j \in N} m_{ij}}\right) - w_i\left(1 - \frac{H(X \mid Y_j)}{H(X)}\right)\alpha_i$$

From the above equation, the utility $u_{ij}(\mathcal{S})$ is a decreasing function of the privacy preference w_i, we have

Proposition 4: $\dfrac{\partial u_{ij}(\mathcal{S})}{\partial w_i} \leq 0.$

Therefore, the more user i is concerned about privacy, the less utility she obtains by sharing the information with j. Clearly, when social benefit is the sole factor taken into account, the share action $\mathcal{S}$ is the optimal action. On the other hand, when privacy risk is the sole factor, the not-share action $\mathcal{N}$ is the optimal one as $u_{ij}(\mathcal{S})$ is always negative.

Differently from the extreme cases above, finding the optimal action that maximises $u_{ij}(\_)$ in real applications under particular circumstances relies on the real values of the parameters in Eq. (2). In the next section, by resorting to simulation techniques, we simulate the values for these parameters by assuming some distributions, and then illustrate the results under different parameter settings which represent different circumstances.

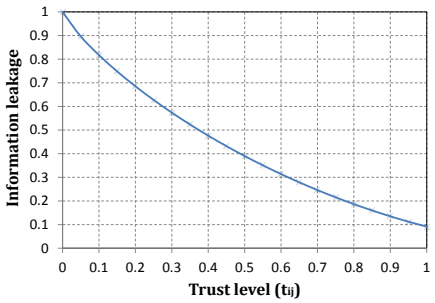
IV. Evaluation

In this section we analyse how trust level and re-sharing probability influence the predicted information leakage, and apply our proposed trade-off model in order to investigate the effectiveness of adaptive sharing, compared with the other two approaches, i.e., always sharing and probabilistic sharing which will be described in §IV-B, with and without the re-share restriction.

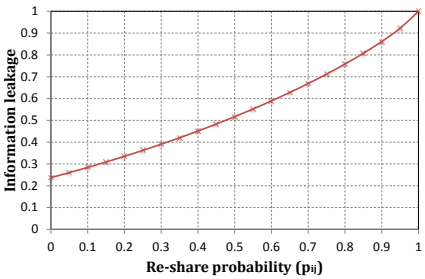
A. On the analysis of information leakage

As discussed in Section III-B, the predicted information leakage of an information-sharing event depends on three parameters: trust level t_{ij}, re-sharing probability p_{ij} and the number k of possible values that $info_i$ indicates. To investigate the influences caused by trust level and re-sharing probability, we set $k = 5$ and vary t_{ij} and p_{ij}.

Figure 2 shows the predicted information leakage changes when the trust level and re-sharing probability respectively increase from zero to one. Information leakage is an increasing function on re-sharing probability, and decreasing function on trust level. Therefore, to mitigate privacy risks, users should share information with friends who have high trust level and low re-sharing probability.



(a) Information leakage decreases as trust level increases. ($p_{ij} = 0.3$)



(b) Information leakage increases as re-sharing probability increases. ($t_{ij} = 0.5$)

Fig. 2: Information leakage as t_{ij} and p_{ij} vary; ($k = 5$).

B. Comparisons among three sharing approaches

To investigate the effectiveness of adaptive sharing, we consider an information-sharing example as described in our motivating scenario (see §II). Here user Alice intends to share her information with her University Friends circle. We extend the number of friends in this selected circle from two to one hundred, that is $N = \{1, \ldots, 100\}$. We consider Alice's weight parameter towards her two types of social benefit $v_i = 0.2$, and the number of possibilities that the information indicates $k = 5$. By assuming a normal distribution, we generate the trust level t_{ij}, re-sharing probability p_{ij}, and average number of interactions m_{ij} ($\in [0, 1]$) for each j in N.

We now describe the three sharing approaches investigated in this example.

- *Always sharing* represents that Alice shares with all of the members in N without considering her potential privacy risks and social benefit.
- *Probabilistic sharing* represents that user i makes the sharing decision Share or Not share depending on a probability (e.g., 0.5 in this example).
- *Adaptive sharing* refers to our solution that Alice shares only with the optimal friends in N.

As shown in Figure 3, adaptive sharing always outperforms the other two approaches. The overall utility of Alice under different privacy preferences is always the greatest, regardless whether the sensitivity of the information is high, or medium, or low. When privacy is the sole utility taken into account (i.e., $w_i = 1$), adaptive sharing prevents the negative utility by adopting the optimal decision Not Share for all of the members. Clearly, if the user only considers her privacy, the best strategy is not disclosing any information. Moreover, the utility difference between adaptive sharing and the other two approaches increases as the sensitivity level of the information increases. Therefore, adaptive sharing saves more loss when the information is highly sensitive.

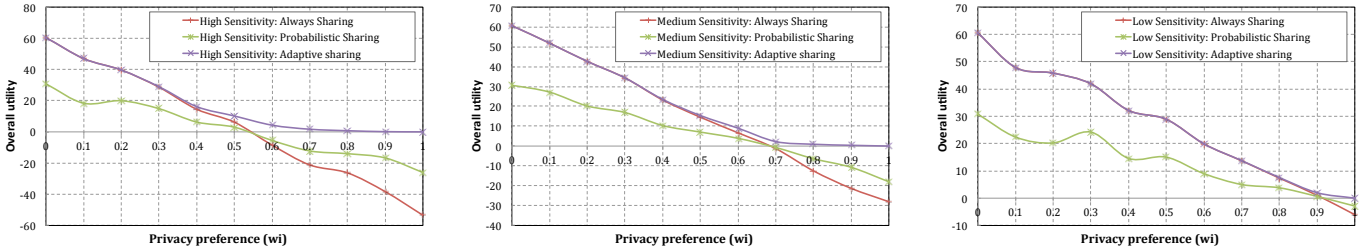
C. Re-share restriction

In order to limit the number of unintended recipients, Facebook currently has a restriction on re-share activity: only mutual friends of the information sharer and re-sharer can see. That is, the information will not flow outside the social connections of the information owner. To make the restriction stronger, we disable re-sharing function to restrict the information within the selected social circle. Due to this restriction, the re-sharing probability p_{ij} in our model becomes zero. We next investigate how the optimal decision changes with the re-share restriction.

We use the same information-sharing scenario as in our previous example, and set $w_i = 0.5$ for simplicity. That is, user Alice views her privacy and social benefit to be equally important. Figure 4a, 4b and 4c depicts Alice's utility of sharing with different members in the selected sharing circle. The x-axis is the identity number of each member in the circle, from 1 to 100, and the y-axis is the corresponding utility. The round markers are the utilities when there is no re-share restriction, while the triangle ones are those with re-share restriction. For utilities which are greater than zero, i.e., markers which are above x-axis, the optimal decision is Share; and Not Share when they are below the axis.

As shown in Figure 4a, when the information is highly sensitive, most markers under the x-axis are in round. That is, re-share restriction makes the user's utility greater (marked in triangle), and fewer members are assigned the decision of Not Share compared with the situation where re-share restriction does not take place. We show respectively the number of markers above and below the x-asix in Figure 5a. With re-share restriction, the optimal decision for 81 members is Share, and the remaining 19 Not Share. When there is no re-share restriction, Share is the optimal decision for only 58 members.

Figure 4b shows that the user's utility of sharing increases when the information is of medium sensitivity. In this case, fewer markers are below the x-axis. When the information is of low sensitivity as shown in Figure 4c, the utilities for all members are greater than zero regardless the re-share restriction, thus for all j, the optimal decision is Share. Therefore, re-share restriction is effective for reducing privacy loss and



(a) High Sensitivity $\alpha_i = 0.9$ (b) Medium Sensitivity $\alpha_i = 0.5$ (c) Low Sensitivity $\alpha_i = 0.1$

Fig. 3: The overall utility of sharing as w_i and α_i vary; ($n = 100$, $v_i = 0.2$, $\forall j, m_{ij} = 50$, $k = 5$).

has more influences on the optimal decision in our adaptive sharing when the information is highly sensitive.

V. Related Work

We have identified several attempts to solve the adaptive sharing problem.

Fabeah, et al. [3] proposed the idea of developing an automated grouping technique that analyzes users' social graph and sharing behaviours, and then identifies new social circles to give users usable and meaningful groupings of friends for sharing their information. This approach enables users to choose a more suitable social circle when they want to share a particular information, but it cannot effectively adapt to users' changing privacy requirement and context as the circles are derived without considering these important factors.

Fang and LeFevre [6] proposed a template for the design of a social networking privacy wizard. The idea is to let users assign "labels" (e.g., share or not share) to a set of selected friends, then by taking these as inputs for their machine learning model, the wizard generates the same (resp. opposite) labels for the other remaining friends who are in the same (resp. different) circle. The wizard asks users' sharing opinions for the selected friends each time users initiate a sharing, and seems to adaptively satisfy users' changing requirements of information-sharing. However, this approach works well under two assumptions: friends in the same social circle bring the user the same consequences of sharing, and users are able to understand the risks of sharing and are fully privacy-aware.

Bilogrevic et al. [4] built an adaptive information-sharing system for mobile social networks. The system uses a machine learning approach to monitor users' sharing decisions under different contexts. Then the system predicts decisions for new sharing requests based on these previous decisions and new context as well. The system also assumes users are fully privacy-aware, but the assumption may not be true for average users in real world and by using this system, users' privacy is not better protected.

In this paper, we focus on a utility-based trade-off framework that models the consequences of sharing into utilities by taking into account users' privacy preferences, social requirements and as well as contextual factors. By evaluating different utilities under different sharing decisions, we obtain an optimal decision and recommend it to users to support their decision-making. Acquisti [2] discussed the economics literature that relates to trading-off the loss against benefit of sharing personal information. Squicciarini and Griffin [14] studied how users decide whether to disclose, share or lie about their information in a game-theoretic approach by evaluating their utilities under these three strategies. In their model, the benefit and loss of sharing are defined as two generalized functions and their evaluations for real applications have not been investigated. Ioannidis, Pym and Williams [7] developed a mathematical model to find the optimal decisions for organizations when they deploy information security policies. This study models the trade-offs among several properties of information security by combining the measurements of these properties into a utility function.

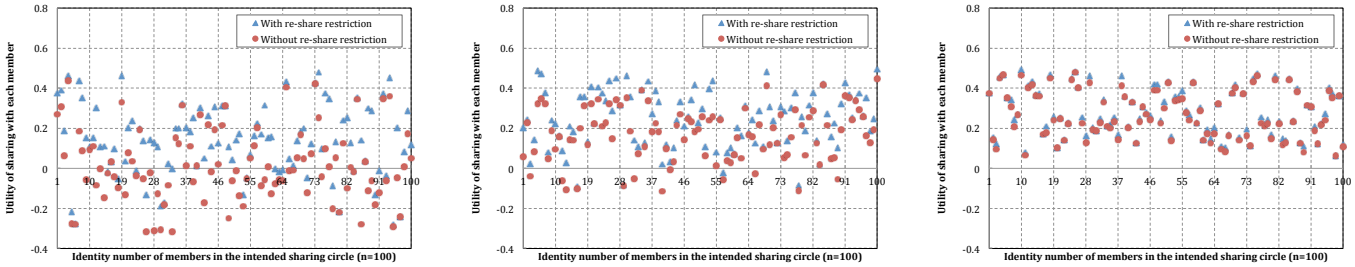
Another challenge explored in this paper is the measurement of privacy risks and social benefit. We try to predict and measure the information leaked to unintended recipients and untrusted friends who cause the potential privacy loss. In this paper, a measuring model is proposed based on Shannon's entropy [12] and combined with the sensitivity of the sharing information, users' privacy loss is computed. A similar work was done by Liu and Terzi [11] and they defined a mathematically sound methodology for computing users' privacy scores of their privacy settings in online social networks. They took the sensitivity of the sharing information as the main factor, and the more sensitive a user shares the lower score the user gets. Unlike this work, we consider the amount of information leakage as also an important and necessary factor. Even though some information has high sensitivity, the potential privacy risk is zero if it is not leaked to any unintended recipients or untrustworthy friends.

VI. Conclusion and Future Work

Privacy management is an important problem in online social networks. Existing privacy control is neither adequate nor effective in adaptively deciding the sharing circles to satisfy users' changing sharing requirements in different contexts.

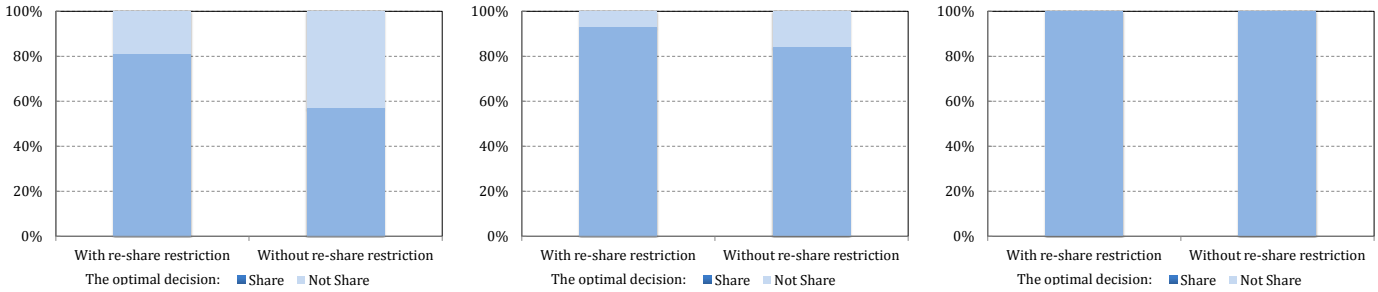
This paper has proposed a utility-based trade-off framework that models and quantifies users' adaptive sharing requirements as utility of potential privacy risks and social benefit. By balancing these two metrics, the proposed framework recommends users a subset of the selected sharing circle each time they initiate an information-sharing action, which can always maximise users' overall utility. Numerical simulations show that our approach of adaptive sharing outperforms "always sharing" and "probabilistic sharing", especially when the information is highly sensitive. The simulations also show that the re-share restriction is effective for protecting privacy.

We plan to extend our approach in the following directions. First, we plan to further investigate adaptive sharing problem



(a) High sensitivity $\alpha_i = 0.9$ (b) Medium sensitivity $\alpha_i = 0.5$ (c) Low sensitivity $\alpha_i = 0.1$

Fig. 4: Utility of sharing with each j, from number 1 to 100.



(a) High sensitivity $\alpha_i = 0.9$ (b) Medium sensitivity $\alpha_i = 0.5$ (c) Low sensitivity $\alpha_i = 0.1$

Fig. 5: The percentage of Share and Not Share.

from a game-theoretic perspective. Specifically, we plan to extend our modelling framework to analyse users' incentives for sharing/not sharing. Second, we plan to investigate how to engineer an adaptive system to realise our adaptive sharing framework. We will explore well established adaptive system engineering theory to investigate how to monitor and assign values to those parameters in our framework, how to do the analysis and decision planning in real social networking systems, how to effectively provide sharing suggestions to users, and how to update the values of parameters after users make final sharing decision. Finally, we plan to implement our framework in a social networking application and evaluate using a user study to investigate users' sharing experiences with and without our adaptive sharing recommendations.

Acknowledgment

This research is funded by ERC advanced grant 291652 and the UK EPSRC. The authors would like to thank Michael Jackson for his comments.

References

[1] Facebook. http://www.facebook.com.

[2] A. Acquisti. Nudging privacy: The behavioral economics of personal information. *IEEE Security & Privacy*, 7(6):82–85, 2009.

[3] F. Adu-Oppong, C. K. Gardiner, A. Kapadia, and P. P. Tsang. Social circles: Tackling privacy in social networks. In *SOUPS*, pages 3–17, 2008.

[4] I. Bilogrevic, K. Huguenin, B. Agir, M. Jadliwala, and J.-P. Hubaux. Adaptive information-sharing for privacy-aware mobile social networks. In *UbiComp*, pages 657–666, 2013.

[5] C. Dwyer, S. R. Hiltz, and K. Passerini. Trust and privacy concern within social networking sites: A comparison of facebook and myspace. In *AMCIS*, page 339, 2007.

[6] L. Fang and K. LeFevre. Privacy wizards for social networking sites. In M. Rappa, P. Jones, J. Freire, and S. Chakrabarti, editors, *WWW*, pages 351–360. ACM, 2010.

[7] C. Ioannidis, D. J. Pym, and J. Williams. Information security trade-offs and optimal patching policies. *European Journal of Operational Research*, 216(2):434–444, 2012.

[8] M. Johnson, S. Egelman, and S. M. Bellovin. Facebook and privacy: It's complicated. In *SOUPS*, pages 9:1–9:15, 2012.

[9] H. Kwak, C. Lee, H. Park, and S. Moon. What is twitter, a social network or a news media? In *WWW*, pages 591–600, 2010.

[10] T. Li and N. Li. On the tradeoff between privacy and utility in data publishing. In *KDD*, pages 517–526, 2009.

[11] K. Liu and E. Terzi. A framework for computing the privacy scores of users in online social networks. In *ICDM*, pages 288–297, 2009.

[12] C. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 623–656, July, October 1948.

[13] M. M. Skeels and J. Grudin. When social networks cross boundaries: A case study of workplace use of facebook and linkedin. In *GROUP*, pages 95–104, 2009.

[14] A. C. Squicciarini and C. Griffin. An informed model of personal information release in social networking sites. In *SOCIALCOM-PASSAT*, pages 636–645, 2012.

[15] F. Stutzman, R. Gross, and A. Acquisti. Silent listeners: The evolution of privacy and disclosure on facebook. *Journal of privacy and confidentiality*, 4(2):2, 2013.

[16] F. Stutzman and J. Kramer-Duffield. Friends only: examining a privacy-enhancing behavior in facebook. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1553–1562. ACM, 2010.

[17] Y. Wang, P. G. Leon, K. Scott, X. Chen, A. Acquisti, and L. F. Cranor. Privacy nudges for social media: an exploratory facebook study. In *WWW (Companion Volume)*, pages 763–770, 2013.

[18] M. Yang, Y. Yu, A. K. Bandara, and B. Nuseibeh. Adaptive Sharing for Online Social Networks: A Trade-off between Privacy Risk and Social Benefit. Technical Report 2014/04, July 2014.