PRIVACY PRESERVING PHOTO SHARING ON SOCIAL NETWORK

M. MATHANRAJ, N.MOHAN, J.HARIRAMAN, R.VIGNESH, M.MARIMUTHU

UG STUDENT, ASSISTANT PROFESSOR, UG STUDENT, UG STUDENT, UG STUDENT.

COMPUTER SCIENCE AND ENGINEERING, St. MOTHER THERESA ENGINEERING COLLEGE, TUTICORIN, INDIA.

Abstract : With the development of social media technologies, sharing photos in online social networks has now become a popular way for users to maintain social connections with others. However, the rich information contained in a photo makes it easier for a malicious viewer to infer sensitive information about those who appear in the photo. How to deal with the privacy disclosure problem incurred by photo sharing has attracted much attention in recent years. When sharing a photo that involves multiple users, the publisher of the photo should take into all related users' privacy into account. In this paper, we propose a trust-based privacy preserving mechanism for sharing such co-owned photos. The basic idea is to anonymize the original photo so that users who may suffer a high privacy loss from the sharing of the photo cannot be identified from the anonymized photo. The privacy loss to a user depends on how much he trusts the receiver of the photo. And the user's trust in the publisher is affected by the privacy loss. The anonymiation result of a photo is controlled by a threshold specified by the publisher. We propose a greedy method for the publisher to tune the threshold, in the purpose of balancing between the privacy preserved by anonymization and the information shared with others. Simulation results demonstrate that the trust-based photo sharing mechanism is helpful to reduce the privacy loss, and the proposed threshold tuning method can bring a good payoff to the user.

Index Terms **- social trust, anonymization, privacy preserving, photo sharing, online social networks.**

I. INTRODUCTION

Social media [1], which enable people to interact with each other by creating and sharing information, has now become an importation part of our daily life. Users of social media services create a huge amount
of information in forms of text posts, digital photos or videos. Such user-generated content Is the lifeblood of social media [2],[3]. However, user generated Content usually involves the create sensitive information, which means the sharing of such content may compromise the creator's privacy. How to deal with the privacy issues caused by information sharing is a long active topic in the study of social media [4], [5].A major form of the content sharing activities in social media websites is the sharing of digital photos. Some popular online social networking services, such as Instagram1, Flicker 2, and Pinterest3, are mainly designed for photo sharing.

1https://www.instagram.com/

2https://www.flickr.com/

3https://www.pinterest.com/

Compared to textual data, photos can deliver more detailed information to the viewer, which is detrimental to individual's privacy. Moreover, the background information contains in a photo may be utilized by a malicious viewer to infer one's sensitive information. On the good side, it is more convenient for a user to hide his sensitive information, without too much damage to insensitive information, by image processing (e.g. blurring) than by text editing. In this paper we study the privacy issue raised by photo sharing in online social networks (OSNs). Privacy policies in current OSNs are mainly about how a user's information will be explored by the service provider, and through which methods a user can control the scope of information sharing. Most OSNs offer a privacy setting function to their users. A user can specify, usually based on his relationships with others, which users are allowed to access the photo he shares. It should be noted that the photo shared by a user may relate to other users. If the sharing of such photos is fully controlled by one user, then the privacy of other related users may be compromised. This privacy issue can be further explained via the following example. Suppose that Alice takes a photo of herself and her friend Bob, and then shares the photo to her colleague Charlie without telling Bob. If Bob does not know Charlie well, then the sharing of the photo will becomes a privacy invasion to Bob. In the above example, the photo is actually co-owned by Alice and Bob. When Alice wants to share the photo with others, she should solicit Bob's opinion, or at least, she should take some measures to reduce the possible privacy loss to Bob. For example, Alice can use a photo editing tool to make Bob's face blurred, so that Bob can hardly be identified by Charlie. Given a photo, or more generally, a data item, related users usually have different opinions on whether a user is allowed to access it. Researchers have proposed different approaches to resolve the conflicts among users' access control policies [7], [8], [9]. In most studies, an aggregated policy, which is essentially a set of users who are authorized to access the data item, will be generated by a mediator (e.g. the service provider). In our previous work [10], a trust-based mechanism is proposed for collaborative privacy manage mention OSNs. The proposed mechanism requires a user to solicit related users' opinions before sharing a data item with others. The trust values between users are utilized to generate an aggregated option. By comparing the aggregated option with a threshold, the user decides whether to share the data item.

Previous studies usually consider the data item to be shared as a whole. That is to say, a user can either obtain all the information contained in the data item or get nothing. However, the aggregated access control policy cannot always make every related user satisfied. In the above example, suppose there is another user David in the photo taken by Alice. If both Alice and David want Charlie to have this photo and Bob does not, then the aggregated policy generated by a majority voting scheme will authorize Charlie to view this photo. As a result, Bob's privacy is still compromised. While in fact, in the case of photo sharing, it is possible to completely resolve conflicts among users' privacy requirements, though it is hard to realize in the case of textual data sharing. The rationale is that

a photo can be divided into multiple disjoint areas. Each area can be correlated to a specific user. If we delete this area or make the area blurred, then the corresponding user's privacy can be preserved when the photo is accessible to an undesired user. In this paper, we consider a photo-sharing scenario where the user who publishes the photo, referred to as publisher, decides how to process the photo so as to protect privacy of related users. A trust-based mechanism is proposed to help the publisher make a proper decision. Different from our previous work [10], the publisher does not communicate with other related users before he posts the photo.

Instead, the publisher predicts the privacy loss to each related user incase that the photo is shared with a certain user. We explore the trust between users to measure the privacy loss. The basic idea is that whether a user allows another user to learn his sensitive information depends on how much the former trusts the latter. Also, whether a user is willing to protect another user's privacy depends on how much the former trusts the latter. Basically, if the publisher predicts a high privacy loss to a related user who is also highly trusted by the publisher, //98then the publisher will "delete" the user from the photo by processing the corresponding area of the photo. Those related users are not directly involved in the decision making process of the publisher. After the photo is processed and sent to the user designated by the publisher, each related user can evaluate whether his privacy is disclosed. If the user suffers a privacy loss, he will lose trust in the publisher. And if the user finds that his privacy is protected by the publisher, he may have more trust in the publisher. Due to the correlation between privacy and trust, the publisher will not ignore other users' privacy when sharing photos. Intuitively, if the publisher deletes all users from the photo, then no one will suffer a privacy loss, and the publisher will gain more trust from others. As a result, the publisher's privacy will be more valued by other users. However, with all user related information being deleted, the sharing of the photo becomes meaningless. In the proposed mechanism, a threshold is introduced to control the number of users deleted from a photo. To find a balance between privacy preserving and photo sharing, we propose a method to make the threshold adaptive to the trust relationship between users. The main contributions of this paper are summarized as follows: a trust-based mechanism is proposed for photo sharing in OSNs. The trust values between users are utilized to determine whether a user's privacy will be protected. The trust values are updated according to the privacy loss, and the proposed mechanism can prevent the user from ignoring other users' privacy. To balance between photo sharing and privacy preserving, we propose a method to tune the threshold that determines the number of users deleted from a photo. We have conducted a series of simulations to demonstrate the effectiveness of the proposed methods. The rest of the paper is organized as follows. Section introduces some studies on the privacy issues of photo sharing. Section III describes the basic model of photo sharing in OSNs and the trust evaluation model. The trust-based photo anonymization approach is presented in Section IV. And the method proposed for threshold tuning is described in Section V. Simulation results are presented in Section VI. Finally, conclusions are drawn in Section VII.

RELATED WORK

\

\A. Privacy Management of Photo Sharing

The sharing of multimedia content has now become quite popular in online social networks. Compared to textual content, multimedia content is more appealing to users [11]. The large-scale and rapid spread of multimedia content may cause a great loss to individual's privacy if the content contains sensitive information about the individual. Specifically, when a user shares a photo with others, all users related to this photo face a risk of privacy disclosure. Researcher has begun to investigate such privacy issues. It is generally believed that the sharing of the photo should be controlled by all the related users. In [12], Yuan et al. proposed a privacy-preserving photo sharing framework which uses visual obfuscation technique to protect users' privacy. When processing a photo, the proposed framework considers both the content and the context of a photo. In [13], Xu et al. designed a mechanism that enables all the related users of a photo participate in the decision-making process of photo sharing. With the help of a facial recognition technique, they developed a distributed consensus-based method to generate the final decision. Based on the encryption algorithm proposed in [14], Ma et al. proposed a key management scheme to authorize and repeal a user's privilege of accessing multimedia data [15].With the help of image processing techniques; we can realize a fine-grained privacy management of photo sharing. In [16], lia et al. proposed an access control model for photo sharing, where a photo is transformed into a set of layers each of which contains a single blurred face. Based on each user's privacy policy, the final photo presented to a viewer is generated by superimposing certain layers. In [17], Lee etal. proposed a multiparty access model for photo sharing in OSNs, where the granularity of access control can be gradually tuned from photo level to face level. In [18], Vishwamitra et al. proposed a collaborative privacy management approach for photo sharing in OSNs. The proposed approach considers the personally identifiable information (PII) items in a photo, and designs a conflict resolution method for PII-level access control policies. The photo sharing mechanism proposed in this paper also aims at a fine-grained privacy protection for users. Different from previous studies, the mechanism proposed in this paper does not utilize the access control policies of related users to make the decision on photo sharing. Instead, the service provider estimates the privacy loss to each related user, and then decides which users' privacy should be preserved.

B. Trust-based Privacy-Preserving Approaches

Trust plays an important role in online social networks [19]. The trust relationship between users has been explored to deal with the access control problem. In the decentralized online social network proposed by [20], a user can tell another user with whom he trusts most to store his profile. Based on the access control policies provide by other users, a user can decide with whom to share the sensitive information. In [21], Rather et al. proposed a trust-based access control model for resource sharing. The model considers the authorization requirements of all related users. And the trust between users is utilized to resolve the conflict among different users' access control policies. In [22], Gay et al. proposed a relationship-based access control mechanism with which users can control how their data are re shared. And they built a trust model to quantify user relationships. In [23], Yu et al. applied deep learning algorithm to determine the privacy settings for photo sharing. During the training of learning models, both the content sensitiveness of the photo and

the trustworthiness of the users with whom the photo is shared are considered. In this paper, we also utilize the trust values to determine with whom a photo can be shared. While different from previous studies, the trust values in the proposed mechanism are associated with users' privacy loss: the privacy loss to a user is dependent on his trust in others, and a user will lose trust of other users if he causes privacy loss to them.

SYSTEM MODEL

A. Graph Representation of an Online Social Network

Consider an online social network (OSN) which consists of N users. The network can be represented by a directed graph G, have with V being the set of vertices and E being the set of edges. Each vertex vi represents a user. Throughout this paper, unless otherwise stated, we use the two terms vertex and user interchangeably to refer to areal entity in an OSN. Given two users vi; vj 2 V (i 6= j), the edge from user vi to user vj (if exists) is denoted as eij . The edge indicates a certain relationship between the two users, e.g. user vi is the employer of user vj . Here in this paper we define that as long as user vi knows user vj , there is an edge eij between them. And we refer to vj as a friend of vi. B. Sharing Co-Owned Photos Suppose that user vi wants to share a sensitive photo d with user vj. We refer to vi as the publisher and vj as the recipient. By sensitive we mean that one or more users can be identified in the photo. We refer to such users as, and denote the set of stakeholders related to a photo d as Sd. When there is more than one user in Sd, we say the photo dis co-owned by the stakeholders. IT that user vi is not necessarily included in Sd. If vi =2 Sd, it is very likely that the photo is originally created by some other user, and wants to share it with a third user vj. The sharing of may disclose privacy of the stakeholders. If the recipient vj himself is a stakeholder of d, which means vj has the right to access d, then vi can share d with vj directly. Otherwise, user vi should, in principle, ask all the stakeholders for permission beforehand. However, different stakeholders generally have different opinions on whether the photo d can be shared to user vj, and it is difficult for the publisher vi to make a decision. An intuitive way to deal with this problem is to treat the photo as a collection of personally identifiable data items fdkgvk2Sd. If a stakeholder vk 2 Sd does not want to the photo to be shared with user vj ,then the publisher vi can just "delete" the corresponding data item dk from d (e.g.by blurring user vk'sface).After this photo anonymization process, the anonymized photo d0 can be sent to the recipient vj .To ease the burden of the publisher and stakeholders, in this paper we require the service provider (SP) of the OSN to do the anonymization work. The basic idea is that the publisher vi first uploads the photo d to the SP. Then, the SP estimates the privacy loss to each stakeholder and determines which stakeholders should be deleted. The recipient will get the anonymized photo d0 from the SP. In Section IV, we will discuss how the trust between users can be utilized in the above process.

B. Trust Evaluation

Trust is generally understood as a subjective concept. To conduct a formal analysis of the impact of trust on users' photo sharing behaviors, we use a scalar to quantify the degree of trust. Given two users vi; vj 2 V (i 6= j), we denote user vi's trust in user vj as tij. And we define 0 _ tij _ 1.A high value of tij indicates user vj is highly trusted by user vi. It should be noted that user vj 's trust in user vi, denoted as tji, is generally different from tij. One user's trust in another is closely related to the type of the relationship between the two users. In out project for example, a user usually trusts his family members more than his colleagues. Moreover, the value of trust constantly changes as the interactions between the two users become more. Specially, one will lose the trust of others if he causes a damage to others in some way. Given the network represented by G, we first utilize the edge information to determine the initial trust values between users. That is, before user vi and user vj interact with each other, tij is set to a positive number if the edge eij exist, otherwise tij is set to 0. Then, tij is updated based on the interactions between the two users. Details of the update rule will be discussed in the following section.

TRUST-BASEDPHOTO ANONYMIZATION

Current OSNs impose no restriction on the sharing of co-owned photos. When a publisher shares a co-owned photo with others, some stakeholders' privacy may be disclosed. To reduce the privacy loss caused by photo sharing, in this section we propose an anonymization mechanism which preserves a stakeholder's privacy by deleting his personally identifiable items from the photo. The key of the proposed mechanism is to associate trust with privacy loss. Next, we first describe the trust-based mechanism and then analyze how this mechanism can motivate a user to protect others' privacy.

A. Associate Trust with Privacy Loss

When user vi wants to share a sensitive photo d with user vj, he first uploads the photo to the SP. It is assumed that all the users appearing in the photo have been tagged by the publisher, or they can be identified by the SP via some face recognition technique. Either way, the SP can determine the stakeholders of the photo. After that, the SP estimates the privacy loss to each stakeholder. For any vk 2 Sd, if the recipient vj is able to identify vk in the photo sent from the SP, user vk may suffer a privacy loss. We use l(d)jk to

denote the loss. Intuitively, the more user vk trusts user vj, the less privacy loss user vk will perceive. The value of l(d)jk also depends on how sensitive, from the perspective of user vk, the photo. The more sensitive the photo is, the more privacy loss user vk will perceive. Therefore, we define l(d)jk. where _ 2 [0; 1] is a constant specified by the SP. Given the estimated privacy loss to each stakeholder, the SP can decide how to anonymize the photo. We use a binary variable pk to indicate whether the stakeholder vk can be identified in the anonymized photo d0. Intuitively, if ~l(d) jk is high, then the SP should delete the identifiable data items of vk from the photo, and there is pk = 0. Considering that it is the publisher vi who wants to share the photo, the SP should also take the publisher's opinion into account when making the decision. To this end, we introduce a parameter i and define the Given the estimated privacy loss to each stakeholder, the SP can decide how to anonymize the photo. We use a binary variable pk to indicate whether the stakeholder vk can be identified in the anonymized photo d0. Intuitively, if ˜ l(d) jk is high, then the SP should delete the identifiable data items of vk from the photo, and there is pk = 0. Considering that it is the publisher vi who wants to share the photo, the SP should also take the publisher's opinion into account when making the decision. To this end, we introduce a parameter θi and define the anonymization rule as According to above rule, the estimated privacy loss ˜ l(d) jk is weighted by the trust value tik. The idea is that the more the publisher vi trusts the stakeholder vk, the more the publisher values his relationship with the stakeholder, and the more the publisher is willing to protect the stakeholder's privacy. The threshold θi ∈ [0,1] indicates how much the publisher vi values other users' privacy. A low value of θi implies that the stakeholders' privacy will be well preserved. In an extreme case where θi = 0, every stakeholder will be deleted from the photo, which means the publisher vi shares no information with the recipient vj. Contrarily, when θi = 1, namely the publisher does not care about others' privacy, the SP will not make any change to the photo. The SP processes the photo d according to{pk}vk∈Sd. Then the SP sends the anonymized photo d0 to the recipient vj. It is assumed that the SP will inform every stakeholder that the photo d0 is accessible to vj. Each stakeholder vk can then evaluate his privacy loss and report the actual loss to the SP. Depending on how much the privacy loss is, the trust of stakeholder vk in the publisher vi, denoted as tki, may increase or decline.

The function f trust (x, y) satisfies: • ∀x ∈ [0,1],∀y ∈ (−∞,∞), there is 0 ≤ f trust (x, y) ≤ 1; • Given x ∈ [0,1], f trust (x, y) is a decreasing function of y; • ∀x ∈ [0,1], if y ≥ 0, then there is f trust (x, y) ≤ x; • ∀x ∈ [0,1], if y ≤ 0, then there is f trust (x, y) ≥ x. According to the update rule defined above, if the stake- holder v k can be identified in the anonymized photo, then he will suffer a privacy loss l(d) j k and lose trust in the publisher vi (i.e. t0ki ≤ t k i). The higher the privacy loss is, the lower the trust value will be. On the contrary, if the stakeholder v k is deleted from the photo, then he will have more trust in the publisher vi (i.e. t0ki ≥ tki), since his privacy is preserved. In such a case, l(d) j k denotes the privacy loss that the stakeholder could have suffered from the sharing of the photo. The more privacy loss the publisher prevents, the more the trust value will increase. To make the update rule works, each stakeholder shall provide a feedback l(d) jk to the SP after the photo is shared, whether he suffers a privacy loss or not. If the stakeholder provides no feedback and we use the main function to make sure that the updated trust value is no larger than 1. As mentioned earlier, before the photo is sent to the recipe-end, the SP can only estimate the privacy loss of a stakeholder to the SP, then the SP just presumes that the stakeholder has no privacy loss v k, since the sensitivity δ(d) k is unknown to the SP. After the photo is sent to the recipient, the SP can infer the value of δ(d) k from the actual privacy loss l(d) jk reported by the stakeholder vk. Later if another user wants to share the photo d, or the recipient vj wants to forward the anonymized photo to a third user, then the SP can use the inferred sensitivity to compute the privacy loss of the corresponding stakeholder. In such a case, the SP can consider each recipient separately. That is, for each recipient, the mechanism proposed above is applied to decide how to anonymize the photo. Given a stakeholder, his trust in the recipients may vary from one to another. Therefore, different recipients may get different versions of anonymized photo. After all the recipients have got the photos, each stakeholder computes his privacy loss, and then the SP can update the trust values.

B. The Motivation of Privacy Protection

The trust relationship between users is thoroughly explored in the photo sharing mechanism described above. On one hand, the trust of a stakeholder in the recipient is utilized to measure the privacy loss of the stakeholder. On the other hand, the trust of the publisher in the stakeholder is utilized to measure how much the publisher cares about the privacy loss to the stakeholder. Moreover, the trust of a stakeholder in the publisher is updated according to privacy loss of the stakeholder. By incorporating trust into the photo anonymization rule (see (4)) and incorporating privacy loss into the Trust update rule (see (5)), we can prevent the users from ignoring the privacy issue when sharing photos with others. As a result, everyone's privacy can be better preserved. In the proposed mechanism, we introduce a threshold θi to quantify how much user vi cares about other users' privacy. If user vi does not care about others' privacy, i.e. θi = 1, then whenever user vi wants to share a photo d related to user vk with a third user, he will cause a privacy loss to vk as long as vk is sensitive to the photo (i.e. δ(d) k > 0). As a result, user vi loses user vk's trust gradually. Suppose that at some point, user vk wants to share a photo ˜ d related to user vi with a third user vj. Since user vk has a low trust in user vi, user vk does not care whether he will cause a privacy loss to user vi, even if user vi is very sensitive to the photo ˜ d and extremely reluctant to show the photo to user vj. As a result, user vi suffers a privacy loss because of the sharing of ˜ d, and his trust in user vk declines. Next time when user vi wants to share a photo related to user vk, if user vk's privacy loss is still ignored by vi, user vk's trust in user vi becomes even lower. From the above discussion we can see that, if a user pays no attention to other users' privacy, then the relation between users will be deteriorating, in the sense that the trust values decline over time. The consequence is that everyone suffers a great privacy loss from the photo sharing activities. Given the proposed photo anonymization rule and the trust update rule, a user who wants to protect his own privacy should also protect another users' privacy by specifying a positive threshold. If user vi sets the threshold θi to a low value, then when he shares a photo, most stakeholders' privacy will be preserved. As a result, user vi gains more trust of the stakeholders. Next time when these stakeholders share photos related to user vi, it is less likely that user vi will suffer a privacy loss. In Section VI, we have conducted a series of simulations to demonstrate the impudence of the threshold on user's privacy loss. When θi is set to 0, user vi will never compromise other users' privacy, which means he will be highly trusted by others and his privacy will be well protected by others. However, in such a case, user vi shares no information with others. This contradicts to the user's intention to join a social network. In the following section we will discuss how to tune the threshold so as to achieve a balance between privacy preserving and photo sharing.

TRADE-OFF BETWEEN PHOTO SHARING AND PRIVACY PRESERVING

The trust-based photo sharing mechanism proposed in the above section encourages users to protect another users' privacy. However, a high degree of photo anonymization causes too much information loss, which has a negative effect on photo sharing. How to make a trade-off between data sharing and privacy preserving has always been an important issue in the study of data privacy [24], [25], [26], [27], [28]. In this section, we first describe how to formulate the publisher's payoff by considering both the privacy loss and the benefit brought by photo sharing. Then we discuss how the publisher should set the threshold θ so as to get a good payoff.

A Payoff to the Publisher

Consider a user vi ∈ V who continually shares photo with others. Suppose that at time point τ ∈ {1,2⋯}, the user wants to share a photo d with user vj. As described in Section IV-A, user vi first uploads the photo to the SP. Then according to the threshold θi set by user vi, the SP can decide how to anonymize the photo. After that, the anonymized photo d0 is published to user vj. The anonymization operation is beneficial to the stakeholders in the sense that the stakeholders' privacy can be preserved. However, anonymization causes information loss, which is not preferred by the publisher vi, since he cannot share the information as he wants to. The more stakeholders the SP deletes from the photo, the less information user vi can share with user vj, and the less satisfaction user vi will feel. where Sd denotes the set of users appearing in the original photo d, Sd0 denotes the set of users appearing in the anonymized photo d0, and |A| denote the cardinality of set A. The benefit ranges from 0 to 1. If there is no stakeholder deleted by the SP (e.g. in the case of θi = 1), user vi can get the maximal benefit. If all the stakeholders are deleted (e.g. in the case of θi = 0), user vi gets zero benefit. Given the photo d, according to the anonymization rule defined in (4), the size of Sd0 is dependent on the threshold θi, user vi's trust in each stakeholder, each stakeholder's trust in user vj, and the sensitivity δ(d) k specified by each stakeholder. That is to say, given a photo d and current trust values between users, the benefit eτ changes with the threshold θi. The sharing of the photo will cause privacy loss to some of the stakeholders. For each stakeholder vk ∈ Sd, his trust in user vi changes after the anonymized photo d0 is published to user vj.

C. Tune the Threshold

From above discussion we know that given the photo d and the trust values between users, the payoff uτ can be seen as a function of the threshold θi. The objective of the user is to and the optimal threshold θ∗ that maximizes the payoff. However, the user cannot solve the optimization problem by himself. For user vi, some of the parameters required to compute the payoff, including the trust values {tki,tkj}vk∈Sd and the sensitivities nδ(d) k ovk∈Sd, cannot be directly observed. Suppose that the SP will tell user vi his current reputation among the stakeholders. Then only after the photo is anonymized and published to user vj, user vi can compute the payoff corresponding to the threshold he has chosen. Considering that the trust values between users are actually evaluated by the SP, we propose the following solution. Considering that the relationship between the threshold and the payoff is complicated and indeterminate, we re- strict the value of the threshold θi is to a finite where K is a positive integer.

As mentioned before, the payoff to user vi is dependent on the sensitivity δ(d) k specified by each stakeholder, and δ(d) k is unknown to the SP, unless the SP has received a privacy loss report from the stakeholder vk. Therefore, as long as there is a stakeholder who has never reported privacy loss to the SP before, the SP cannot determine the analytical form of the payoff function, not to mention deriving the optimal threshold. In addition to discrediting the threshold, we make another implication. Given a photo d, the sensitivity δ(d) k indicates how much the stakeholder vk is sensitive to the photo. The sensitivity is not only user-specific, but also data-specific. If user vi wants to share another photo ˜ d related to vk at time ˜ τ, the SP cannot use the sensitivity δ(d) k inferred from user vk's privacy loss reported at time τ to compute the privacy loss of vk at time ˜ τ, since generally δ(˜ d) k is different from δ(d) k . Due to the data-specific property, the information that the SP learns from the past is of little help to the choice of the threshold for new photos. Nevertheless, we can explore the user-specific property to make past experience useful. We assume that given a user vk, the sensitivity δ(d) k corresponding to any photo d follows the same probability distribution. The expected value of δ(d) k , denoted as δk, indicates how much user vk cares about his own privacy. We refer to δk as the user's sensitivity. When searching the optimal threshold, we replace the data- specific δ(d) k in (2) with the data-independent δk. With this approximation, the SP can use the information learnt from past to compute the privacy loss of stakeholders and the payoff to the publisher. When a user, say vk, reports a privacy loss to the SP for the first time, the SP computes the sensitivity δk by using the reported loss and vk's trust in the recipient. Next time when user vk becomes a stakeholder of some photo, the SP can determine user vk's privacy loss before the photo is published to the designated recipient. With above simplifications, the SP can and a proper thresh- old θi for user vi whenever vi wants to share a photo. The SP maintains a hash table which consists of users who have reported privacy loss and their sensitivity values. Given a photo d to be shared at time τ and the corresponding stakeholders Sd, the SP first computes a payoff ˜ uτ (θ) for each θ ∈ Θ, and then chooses the optimal one θ∗, argmax θ ˜ uτ (θ). To compute the payoff, the SP needs to predict the privacy loss to each stakeholder. Given vk ∈ Sd, the SP checks if vk exists in the hash table. If exists, the SP uses the corresponding sensitivity δk to computes the privacy loss to vk. Otherwise, the SP uses a pre-specified constant δ to estimate the privacy loss. It should be noted that the privacy loss computed by the SP is not necessarily equal to the actual loss perceived by the stakeholder, since the stakeholder's sensitivity may not be known by the SP. Hence, the payoff ˜ uτ (θ) computed by the SP is different from the actual payoff obtained by the publisher vi, unless all the

stakeholders in Sd have been recorded in the hash table. And the optimal threshold θ∗ may be different from the actual one θ∗∗ , argmax θ uτ (θ). The threshold θ∗ chosen by the SP is provided to user vi as a reference. User vi determines θi in a stochastic way: set θi to a value randomly chosen from Θ with a certain probability. Based on the user's final decision θi, the SP conducts photo anonymization and sends the anonymized photo to the designated recipient. After receiving privacy loss reports from stakeholders, the SP updates the hash table by adding a new pair (vk, δk) where δk is the inferred senstivity of user vk.

VI. SIMULATION

To deal with the privacy issue caused by the sharing of co-owned photos in online social networks, we propose a trust-based photo sharing mechanism in Section IV. And to make a better trade-off between photo sharing and privacy preserving, we propose a service provider-assisted method to adaptively tune the threshold that determines how the photo will be anonymized. In order to evaluate the feasibility and effectiveness of the proposed approaches, we conduct a series of simulations on both synthetic and real-world social networks. In this section, we first describe how the networks are constructed and how the simulation environment is set. Then we present the simulation results of the photo sharing mechanism. After that, we describe how to simulate the tuning process of the threshold and present the simulation results.

A. Experiment Setting

Dataset: Simulations are conducted on both synthetic data and real-world data. As we've done in [29], we generate a scale-free network and a small-world network with the help of the mat lab package developed by much nik [30]. Both of the two networks consist of 1000 nodes. The average node degree of each network is 20. There are 20021 undirected edges in the scale-free network and 20000 undirected edges in the small-world network. The real-world data come from Stanford large network dataset collection [31]. The face book dataset is chosen for simulation. The network consists of 1133 nodes and 10902 undirected edges. The average node degree is about 19. 2) Trust Initialization: Given a network, we initialize the trust values between users via two different approaches. The first approach utilizes the transitivity property of trust [32] to determine the initial trust value. Specifically, for any two users vi and vj, the initial value of tij is set to 0.8dij, where dij denotes the length of the shortest path between the two users. If there is no path between them, namely the two users are disconnected, the initial value of tij is set to 0. Though this distance-based approach sets tij and tji to the same initial value, as time goes by, the two trust values will become different, since tij is affected by user vj's behavior and tji is affected by user vi's behavior. The second initialization approach is to set tij to a value chosen from [0,1] uniformly at random, for any pair of vi and vj. In such a case, tij and tij generally have different initial values. Experiment Setup: To simulate the trust-based mechanism proposed in IV, first we need to setup the photo sharing scenario for a given network. We consider a discrete time model. At each time point τ ∈ we randomly select a group users as the publishers. The number of the publishers is given by ρN, where N denotes the total number of users in the network, and ρ ∈ [0,1] is a tunable parameter. For each publisher p, the photo that he wants to share is rep- resented by the stakeholders and corresponding sensitivities. The stakeholders are randomly selected from all users. And we define that the number of stakeholders is at most 20, since the average node degree of the network is 20 or so. Each stakeholder's sensitivity with respect to the photo is chosen from [0,1] uniformly at random. The recipient of the photo is randomly selected from the set of the publisher's friends. Considering that the recipient may re share the photo with other users, we construct a forward chain for the photo published by p. The publisher p, which is the head of the forward chain, is followed by the recipient r1. And the recipient r1 is followed by a user r2 randomly chosen from the set Fr1\{p}, where Fr1 denotes the set of r1's friends. This means that user r1 will forward the photo to r2. User r2 is followed by a user r3 randomly chosen from the set Fr2\{p,r1}, and so on. The length of the forward chain, denoted as Lf, is pre-specified.

C. Trust-based Photo Anonymization

We simulate the trust-based mechanism proposed in Section IV via the following way. Given a network, we first use the method described above to determine the initial trust values and setup the photo sharing scenario. The threshold used in the proposed mechanism is chosen from the set Θ , {0,0.05,0.1,⋯ ,0.45,0.5}. Given any θ ∈ Θ, we set the threshold of every user to θ, and then simulate the photo sharing activities of users. At each time point τ ∈{1,2,...,T}, given a publisher and the corresponding recipient, we first estimate the privacy loss to each stakeholder by using a constant sensitivity δ. Then by comparing the privacy loss to θ, we determine whether a stakeholder should appear in the anonymized photo. After that, we compute the actual privacy loss to each stakeholder by using the random sensitivity chosen in the setup phase. The trust values are updated accordingly. For every user in the network we compute his privacy loss caused by the sharing behaviors of others. Each user's privacy loss is accumulated over time. After the simulation process finishes, we record the average of accumulated privacy loss as the simulation result. To further demonstrate the effectiveness of the proposed trust-based mechanism, we design a photo sharing mechanism which is slightly different from the one proposed in Section.

This mechanism does not utilize the trust values to make the photo anonymization decisions. Instead, given a photo, we randomly select a number of stakeholders and delete them from the photo. The number of deleted stakeholders is equal to that determined by the trust-based mechanism for the same publisher and the same photo. We refer to this mechanism as Random Choose. By comparing the simulation results of the two mechanisms, we can find out whether it is necessary to utilize trust values. Fig. 2 and Fig. 3 show the simulation results obtained under the following setting: T = 100, Lf = 10, ρ = 0.5, and δ = 0.5. As we can see, the average privacy loss always increases with θ, which implies that users who care more about others' privacy will suffer less privacy loss than those who care

less. And compared to the Random Choose mechanism, the trust-based mechanism generally leads to a lower privacy loss. This result demonstrates that the trust-based mechanism can encourage a user to protect other users' privacy, so that everyone's privacy can be better preserved. And from Fig. 2 and Fig. 3 we can see that, when the threshold θ approaches to 0 or 0.5, the advantage of the trust-based method becomes less significant. According to (2), (3) and (4), the expected value of the trust weighted privacy loss is 0.125 when we set the sensitivity δ to 0.5. When θ is high, say 0.5, almost every stakeholder will still appear in the published photo. That is, for every stakeholder vk, it is very likely that pk = 1. Contrarily, when θ is set to a very low value, say 0, every stakeholder will be deleted from the photo. That is, there is pk = 0 for every stakeholder vk. In both of the above cases, the trust values between users have little impudence on the decisions made by the publisher. Therefore, the trust-based method has no significant advantage over the Random Choose method. In the Random Choose mechanism described above, we require the number of stakeholders deleted from a photo to be equal to that in the trust-based mechanism. Here we propose a third mechanism, referred to as All Random, to further demonstrate the effectiveness of the trust-based mechanism. Given a photo and the corresponding stakeholders, the All Random mechanism randomly deletes some stakeholders from the photo. The number of deleted stakeholders is also random. To compare the trust-based mechanism and the All Random mechanism, we fix the threshold used in the trust-based mechanism to 0.125 which is the expected value of the trust- weighted privacy loss (see (4)). The simulation process is similar as before. To better observe the difference between the two mechanisms, we randomly select 3 users. For each user we compute the average privacy loss to the user. Fig. 4 shows the simulation results under the following setting: T = 100, Lf = 10, ρ = 0.5, θ = 0.125, and δ = 0.5. As we can see, compared to the All Random mechanism, the trust-based mechanism leads to a lower privacy loss. This result again demonstrates the advantage of the use of trust. In above simulations, the sensitivity of each stakeholder with respect to a photo is set to a value randomly chosen from [0,1]. Given a photo, the sensitivity varies from one stakeholder to another. To observe how the sensitivities affect the sharing of photos, we conduct the following simulation. Given a network, we first initialize the trust. When setting up the photo sharing scenario, we fix the sensitivity of a stakeholder with respect to a photo to 0.5. The simulation process is similar as before. Fig. 5 shows the simulation results under the setting T = 100, Lf = 10, and ρ = 0.5. As we can see, compared to the case where sensitivity is set to a fixed value, the proposed trust-based mechanism can even lead to a lower privacy loss when the sensitivity varies from one user to another. In fact, the random setting is more realistic than the fixed setting. Hence the simulation result implies that the proposed mechanism can be well applied in practice.

D. Tuning the Threshold

In above simulations, the threshold of each user is set to the same value in all time points. And the simulation results show that a high value of threshold is beneficial to the user in terms of privacy, while it impedes the information sharing between users. In Section V we have proposed a method for the user to set the threshold adaptively so as to keep a balance between privacy preserving and information sharing. To verify the effectiveness of the proposed approach, we conduct the following simulation. Given a network, the parameters and a user vi selected from the network, we first create an "ego" network for the user by selecting the user's friends and friends of friends from the network. For any two users vi and vj in this ego network, the trust tij is initialized to a value chosen from [0,1] uniformly at random. The sensitivity of each user in the ego network is set to a value chosen from [0,1] uniformly at random. At time point $\tau \in \{1,2,\cdots,T\}$, user vi randomly selects a friend vj as the recipient of a photo d. The stakeholders are randomly selected from the ego network. And to simulate the learning ability of the SP, we replace half of the stakeholders with those selected at time $\tau - 1$.We compute the payoff to user vi by using the method described in Section V. Then an "optimal" threshold $\theta*$ can be determined. With probability $1 -$, the threshold θi is set to $\theta*$; with probability , θi is randomly chosen from the set0, 1 K, 2 K,⋯ ,1 . After θi is determined, we simulate the photo anonymization process and compute the actual payoff to user vi. The performance of the threshold tuning method is evaluated by the accumulated payoff. To further demonstrate the performance of the proposed method, here we use two simple methods as references. The first method is to set the threshold. We refer to this method as Fixed. The second method is to randomly choose a threshold from at each time point. We refer to this method as Random. The method proposed in Section V is referred to as -Greedy. During the simulation, we first create the ego network, and set the initial trust values and users' sensitivities as described above. After the recipient and the stakeholders of a photo are determined, we use the three methods mentioned above to set the threshold respectively. The payoff produced by each method is recorded for comparison. Specifically, for the Fixed method, we test all possible values of the threshold and use the best result (i.e. the maximal accumulated payoff) for comparison. Similarly, for the -Greedy method, we test different values of : from 0 to 1 in steps of 0.1. And the best result is used for comparison. The above simulation process is repeated for 10 times so as to the reduce the effect of randomness. As we can see, the - Greedy method always show better performance than the other two methods. This result demonstrates that the information that the SP learns from past interactions with users can help the publisher to chooses a better threshold. The Fixed method performs worst among the three methods, which indicates that it is necessary for the publisher to adjust the threshold when sharing a new photo.

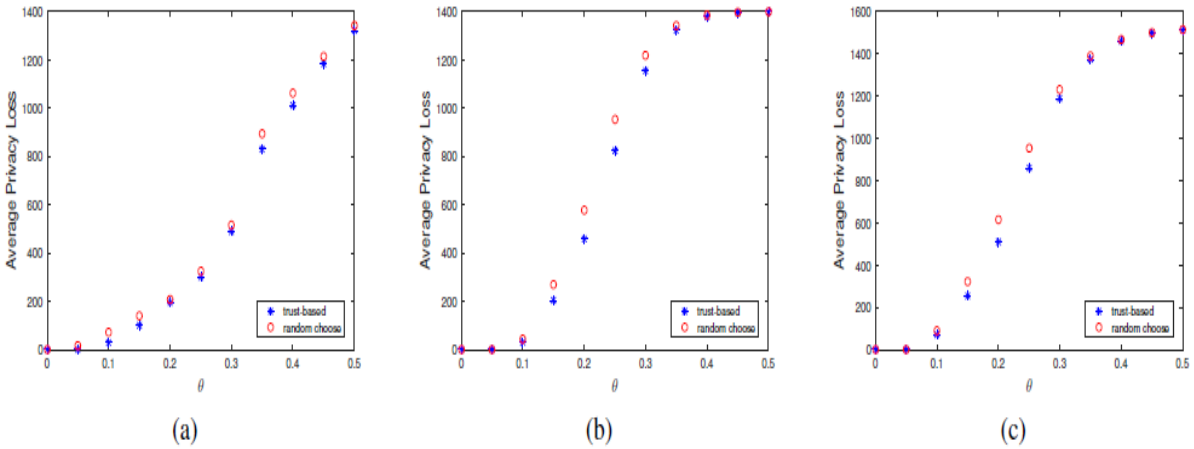

Fig. 2. Simulation results of photo sharing mechanisms. The initial trust between two users is set based on the length of the shortest path between them. The sensitivity of a stakeholder with respect to a photo is set to a random value chosen from [0,1]. The blue stars denote the results obtained by the trust-based mechanism. The red circles denote the results obtained by the Random Choose mechanism. (a) Scale-Free. (b) Small-World. (c) Face book.

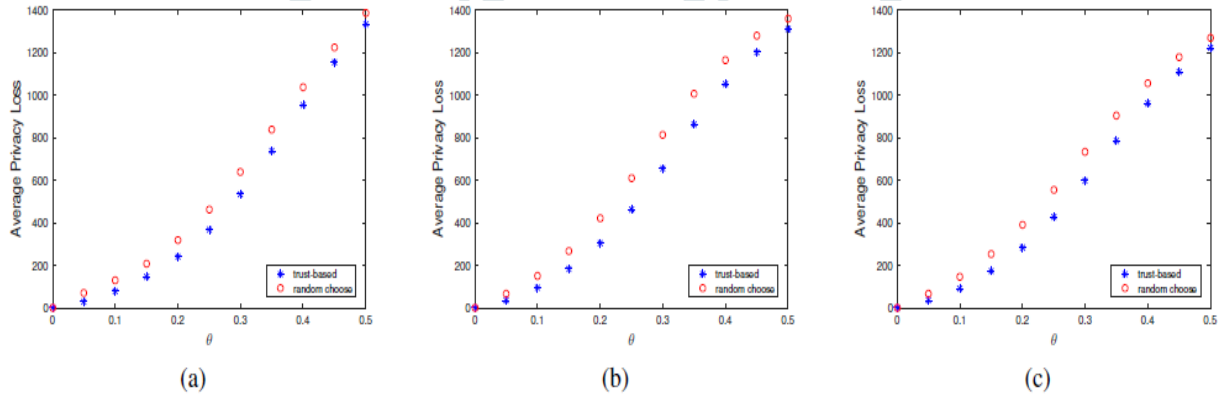

Fig. 3. Simulation results of photo sharing mechanisms. The initial trust between two users is set to a random value chosen from [0,1]. The sensitivity of a stakeholder with respect to a photo is set to a random value chosen from [0,1]. The blue stars denote the results obtained by the trust-based mechanism. The red circles denote the results obtained by the Random Choose mechanism. (a) Scale-Free. (b) Small-World. (c) Face book.

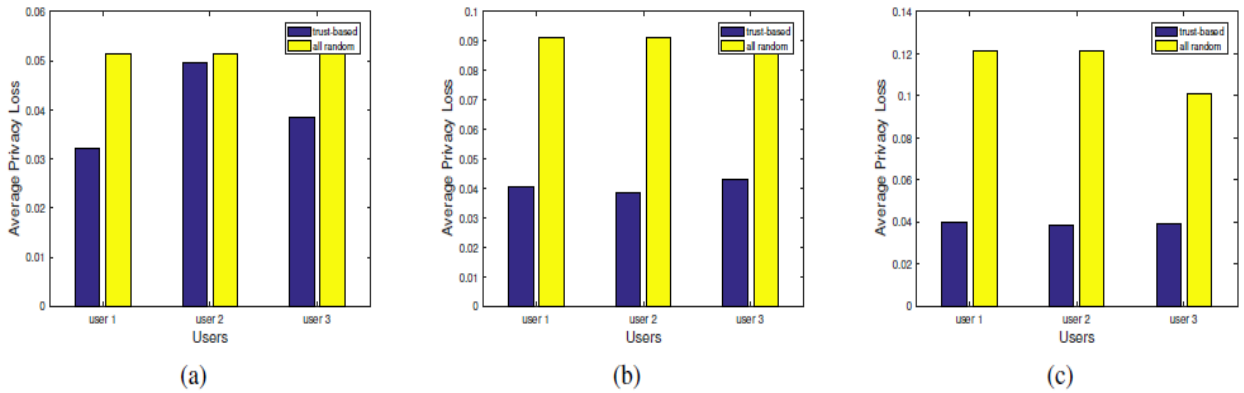

Fig. 4. A comparison of the trust-based mechanism and the All Random mechanism. The initial trust between two users is set to a random value chosen from [0,1]. (a) Scale-Free. (b) Small-World. (c) Face book.

in the ego network is set to a value chosen from [0,1] uniformly at random. At time point $\tau \in \{1,2, \cdots, T\}$, user vi randomly selects a friend vj as the recipient of a photo d. The stakeholders are randomly selected from the ego network. And to simulate the learning ability of the SP, we replace half of the stakeholders with those selected at time $\tau - 1$. Then for each, we compute the payoff to user vi by using the method described in Section V. Then an "optimal" threshold $\theta*$ can be determined. With probability, the threshold θi is set to $\theta*$; with probability, θi is randomly chosen from the s. After θi is determined, we simulate the photo anonymization process and compute the actual payoff to user vi. The performance of

the threshold tuning method is evaluated by the accumulated payoff. To further demonstrate the performance of the proposed method, here we use two simple methods as references. The first method is to set the threshold to a fixed value $\theta \in 0, 1\ K, 2\ K, \cdots, 1$. We refer to this method as Fixed. The second method is to randomly choose a threshold from 0, 1 K, 2 K, ⋯ ,1 at each time point. We refer to this method as Random. The method proposed in Section V is referred to as -Greedy. During the simulation, we first create the ego network, and set the initial trust values and users' sensitivities as described above. After the recipient and the stakeholders of a photo are determined, we use the three methods mentioned

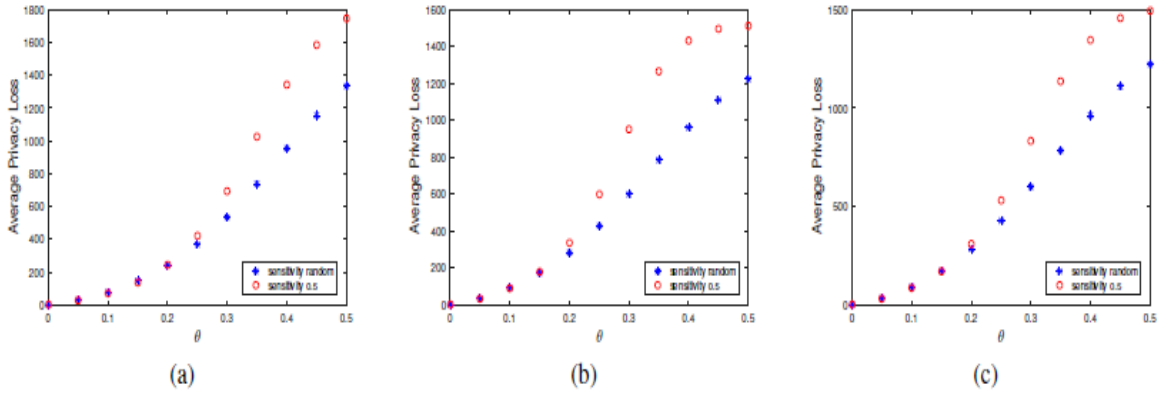

Fig. 5. Simulation results of the trust-based photo sharing mechanism. The initial trust between two users is set to a random value chosen from [0,1].

above to set the threshold respectively. The payoff produced by each method is recorded for comparison. Specifically, for the Fixed method, we test all possible values of the threshold and use the best result (i.e. the maximal accumulated payoff) for comparison. Similarly, for the -Greedy method, we test different values of : from 0 to 1 in steps of 0.1. And the best result is used for comparison. The above simulation process is repeated for 10 times so as to the reduce the effect of randomness. Given a network, we choose 5 users and run the above simulation for each of them. Fig. 6 shows the simulation results under the setting T = 300, K = 10, δ = 0.5. Fig. 7 shows the results under the same setting except that the sensitivity is set to a random value. As we can see, the Greedy method always shows better performance than the other two methods. This result demonstrates that the information that the SP learns from past interactions with users can help the publisher to choose a better threshold. The Fixed method performs worst among the three methods, which indicates that it is necessary for the publisher to adjust the threshold when sharing a new photo. This result also suggests that when the publisher wants to share the same photo to different recipients, the publisher should set different thresholds for different recipients. During the simulation of the Fixed method, we have tried all possible values of the threshold. In each run, we record the best threshold that produces the maximal accumulated payoff. After 10 runs, we find the threshold that is most frequently selected as the best. According to the results shown in Table I, if the user does not want to reset the threshold every time, he shares a photo, he may set the threshold to 0.6 or 0.7, which can bring him a fair payoff. During the simulation of the Greedy method, we have tried 11 values of. In each run, we record the best that produces the maximal accumulated payoff. After 10 runs, we find the one that is most frequently selected as the best. According to the results shown in Table II, the user should not always be greedy, namely following the suggestion made by the SP. Since the privacy loss estimated by the SP is not always correct, a certain randomness is necessary for the user to get a good payoff.

TABLE-1
THE BES THRESHOLD FOR THE FIXED METHOD

	Scale-Free	Small-World	Face book
User 1	0.6	0.7	0.6
User 2	0.6	0.7	0.6
User 3	0.6	0.7	0.6
User 4	0.6	0.6	0.7
User 5	0.6	0.6	0.6

TABLE-2
THE BEST FOR THE GREEDY METHOD

	Scale-Free	Small-World	Face book
User 1	0.7	0.8	0.8
User 2	0.6	0.6	0.6
User 3	0.6	0.7	0.7
User 4	0.7	0.6	0.7
User 5	0.7	0.7	0.8

CONCLUSION

Sharing one co-owned photo in an OSN may compromise multiple users' privacy. To deal with such a privacy issue, in this paper we propose a privacy-preserving photo sharing mechanism which utilizes trust values to decide how a photo should be anonymized. The photo that a user wants to share is temporarily holder by the service provider. Based on the trust relationship between users, the service provider estimates how much privacy loss the sharing of the photo can bring to a stakeholder. Then by comparing the privacy loss with a threshold specified by the publisher, the service provider decides if a stakeholder should be deleted from the photo. After the photo is shared, each stakeholder evaluates the privacy loss he has really suffered, and his trust in the publisher changes accordingly. This trust-based mechanism motivates the publisher to protect the stakeholders' privacy. However, the anonymization operation leads a loss in the shared information. Considering that the threshold specified by the publisher and information sharing. We propose a service provider assisted method to help the publisher to tune the threshold. By using synthetic network data and real-world network data, we conduct a series of simulations to verify the proposed photo sharing mechanism and the threshold tuning method. Simulation results demonstrate that incorporating trust values into the photo anonymization process can help to reduce user's privacy loss, and adaptively setting the threshold is necessary for the publisher to balance between privacy preserving and photo sharing. In current study, we mainly focus on the sharing between one publisher and one receiver. Considering that in practice, a user generally shares a photo with multiple users simultaneously, we'd like to investigate such a one-to-many case in future work. The proposed threshold tuning method can be seen as a greedy method, in the sense that the publisher prefers to choose the threshold that brings him the maximal instant payoff. Due to the correlation between privacy loss and trust values, current choice of the threshold will affect the publisher's future payoffs. In future work, we'd like to investigate how to modify the tuning method so as to achieve a better result.

ACKNOWLEDGMENT

This work was supported by Natural Science Foundation of China (Grant No. 61871037 and No. 61571300). This work was supported by Beijing Institute of Technology Research Fund Program for Young Scholars.

REFERENCES

1) W. G. Mangold and D. J. Faulds, "Socialmedia: The new hybrid element of thepromotion mix," Business horizons, vol. 52, no. 4, pp. 357–365, 2009.
2) A. M. Kaplan and M. Hoenlein, "Users of the world, unite! the challenges and opportunities of socialmedia," Business horizons, vol.53, no. 1, pp. 59–68, 2010.
3) J. A. Obar and S. S. Wildman, "Social media definition and the governance challenge-an introduction to the special issue," 2015.
4) L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, "Information security in big data: data mining," IEEE Access, vol. 2, pp. 1149–1176.
5) S. K. N, S. K, and D. K, "On privacy and security in social media a comprehensive study," Procedia Computer Science, vol. 78, pp. 114 – 119, 2016, 1st International Conference on Information Security and Privacy 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050916000211
6) Fiesler,M.Dye,J.L.Feuston, C. Hiruncharoenvate, C. Hutto, S. Morrison, P. Khan pour Roshan, U. Pavalanathan, A. S. Brackman, M. De Choudhury, and E. Gilbert, "What (or who) is public?: Privacy settings and social media content sharing," in Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing, March 2017, pp. 567–580.
7) Squicciarini, M. Shehab, and F. Paci, "Collective privacy management in social networks," in Proceedings of the 18th ACM International Conference on World Wide Web, April 2009, pp. 521–530.
8) H. Hu, G.-J. Ahn, and J. Jorgensen, "Detecting and resolving privacy conflicts for collaborative data sharing in online social networks," in Proceedings of the 27th ACM Annual Computer Security Applications Conference, December 2011, pp. 103–112.
9) J. M. Such and N. Criado, "Resolving multi-party privacy conflicts in social media," IEEE Transactions on Knowledge and Data Engineering, vol. 28, no. 7, pp. 1851–1863, July 2016.
10) L. Xu, C. Jiang, Y. Qian, Y. Zhao, J. Li, and Y. Ren, "Dynamic privacy pricing: A multi-armed bandit approach with time-variant rewards," IEEE Transactions on Information Forensics and Security, vol. 12, no. 2, pp. 271–285, February 2017.
11) M. Duggan and J. Brenner, "The demographics of social media users 2012," 2013.

12) L. Yuan, P. Korshunov, and T. Ebrahimi, "Privacy-preserving photo sharing based on a secure jpeg," in Computer Communications Workshops, 2015, pp. 185–190.
13) K. Xu, Y. Guo, L. Guo, Y. Fang, and X. Li, "My privacy my decision: Control of photo sharing on online social networks," IEEE Transactions on Dependable and Secure Computing, vol. 14, no. 2, pp. 199–210, March 2017.
14) J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in IEEE Symposium on Security and Privacy, 2007, pp. 321–334.
15) C. Ma, Z. Yan, and C. W. Chen, "Scalable access control for privacy aware media sharing," IEEE Transactions on Multimedia, pp. 1–1, 2018.
16) P. Ilia, I. Polakis, E. Athanasopoulos, F. Maggi, and S. Ioannidis, "Face/off: Preventing privacy leakage from photos in social networks,"
17) L.Chao,W.Wang,andY.Guo,"Afinegrainedmultipartyaccesscontrol model for photo sharing in osns," in IEEE First International Conference on Data Science in Cyberspace, 2016, pp. 440–445.
18) W. Sherchan, S. Nepal, and C. Paris, "A survey of trust in social networks," ACM Computing Surveys, vol. 45, no. 4, pp. 47:1–47:33, August 2013.
19) A. Datta, S. Buchegger, L. H. Vu, T. Strufe, and K. Rzadca, Decentralized Online Social Networks, 2010.
20) N. C. Rathore and S. Tripathy, "A trust-based collaborative access controlmodelwithpolicyaggregationforonlinesocialnetworks," Social Network Analysis and Mining, vol. 7, no. 1, p. 7, 2017.
21) R. Gay, J. Hu, H. Mantel, and S. Mazaheri, "Relationship-based access control for resharing in decentralized online social networks," in International Symposium on Foundations and Practice of Security, 2017, pp. 18–34.
22) J. Yu, Z. Kuang, B. Zhang, W. Zhang, D. Lin, and J. Fan, "Leveraging content sensitiveness and user trustworthiness to recommend finegrained privacy settings for social image sharing," IEEE Transactions on Information Forensics and Security, vol. 13, no. 5, pp. 1317–1332, 2018.
23) L. Xu, C. Jiang, Y. Chen, Y. Ren, and K. J. R. Liu, "Privacy or utility in data collection? a contract theoretic approach," IEEE Journal of Selected Topics in Signal Processing, vol. 9, no. 7, pp. 1256–1269, 2015.
24) Z. Su, Y. Wang, Q. Xu, M. Fei, Y. Tian, and N. Zhang, "A secure charging scheme for electric vehicles with smart communities in energy blockchain," IEEE Internet of Things Journal, pp. 1–1, 2018.
25) L. Xu, C. Jiang, Y. Chen, Y. Ren, and K. J. R. Liu, "User participation in collaborative filtering-based recommendation systems: A game theoretic approach," IEEE Transactions on Cybernetics, vol. PP, no. 99, pp. 1–14, 2018.
26) Z. Su, Y. Hui, and T. H. Luan, "Distributed task allocation to enable collaborative autonomous driving with network softwarization," IEEE Journal on Selected Areas in Communications, vol. 36, no. 10, pp. 2175– 2189, Oct 2018.
27) Q. Xu, Z. Su, Q. Zheng, M. Luo, B. Dong, and K. Zhang, "Game theoretical secure caching scheme in multi-homing edge computingenabled heterogeneous networks," IEEE Internet of Things Journal, pp. 1–1, 2018.
28) L. Xu, C. Jiang, N. He, Z. Han, and A. Benslimane, "Trust-based collaborative privacy management in online social networks," IEEE Transactions on Information Forensics and Security, vol. 14, no. 1, pp. 48–60, Jan 2019. [30] L. Muchnik, "Complex networks package for mat lab," 2013. [Online]. Available: http://www.levmuchnik.net/index.html
29) J. Leskovec and A. Krevl, "SNAP Datasets: Stanford large network dataset collection," http://snap.stanford.edu/data, June 2014.
O. Richters and T. P. Peixoto, "Trust transitivity in social networks," PLOS ONE, vol. 6, no. 4, pp. 1–14, 04 2011. [Online]. Available: https://doi.org/10.1371/journal.pone.0018