International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Enhanced Multi-party Privacy Conflicts in Social Media

BH Sravitha

M.Tech, Department of Computer Science and Technology, SRKR Engineering College, Bhimavaram, West Godavari, Andhra Pradesh, India

ABSTRACT

Items shared through Social Media may affect more than one user's privacy e.g., photos that depict multiple users, comments that mention multiple users, events in which multiple users are invited, etc. The lack of multi-party privacy management support in current mainstream Social Media infrastructures makes users unable to appropriately control to whom these items are actually shared or not. Computational mechanisms that are able to merge the privacy preferences of multiple users into a single policy for an item can help solve this problem. However, merging multiple users' privacy preferences is not an easy task, because privacy preferences may conflict, so methods to resolve conflicts are needed. Moreover, these methods need to consider how users' would actually reach an agreement about a solution to the conflict in order to propose solutions that can be acceptable by all of the users affected by the item to be shared. Current approaches are either too demanding or only consider fixed ways of aggregating privacy preferences. In this paper, we propose the first computational mechanism to resolve conflicts for multi-party privacy management in Social Media that is able to adapt to different situations by modeling the concessions that users make to reach a solution to the conflicts. We also present results of a user study in which our proposed mechanism outperformed other existing approaches in terms of how many times each approach matched users' behavior.

Keywords: Social Media, OSN, Majority Voting, Veto Voting

I. INTRODUCTION

Social media sites have an extensive presence in nowadays society. User can learn a lot of useful information about human behavior and interaction by paying attention to the information and relations of social media users. This information can be open or private. Ensuring the private data of the clients in informal organizations is a genuine concern. It proposes different method to solve these privacy conflicts. As of late we have been viewing a huge increment in the development of on-line social systems. OSNs empower individuals to share individual and open data and make social associations with companions, relatives and different people or groups. Notwithstanding the fast increment in the utilization of interpersonal organization, it raises various security and protection issues. While OSNs permit clients to confine access to shared information, they as of now don't give any component to thoroughly authorize security issue solver connected with different clients. The proposed technique executes an answer for encourage cooperative administration of regular information thing in OSNs. Every controller of the information thing can set his security settings to the mutual information thing. The proposed technique likewise distinguishes protection clashing portions and aides in determining the security clashes and an ultimate choice is made regardless of whether to give access to the mutual information thing.

II. Existing System

Very recent related literature proposed mechanisms to resolve multi-party privacy conflicts in social media. Some of them need too much human intervention during the conflict resolution process, by requiring users to solve the conflicts manually or close to manually; e.g., participating in difficult-to comprehend auctions for each and every co-owned item. Other approaches to resolve multi-party privacy conflicts are more automated, but they only consider one fixed way

of aggregating user's privacy preferences (e.g., veto voting) without considering how users would actually achieve compromise and the concessions they might be willing to make to achieve it depending on the specific situation.

Only considers more than one way of aggregating users' privacy preferences, but the user that uploads the item chooses the aggregation method to be applied, which becomes a unilateral decision without considering the preferences of the others.

Disadvantages:
Computational mechanisms that can automate the negotiation process have been identified as one of the biggest gaps in privacy management in social media.
The main challenge is to propose solutions that can be accepted most of the time by all the users involved in an item (e.g., all users depicted in a photo), so that users are forced to negotiate manually as little as possible, thus minimizing the burden on the user to resolve multi-party privacy conflicts.

III. Problem Statement

Given a set of negotiating users N = {n1, . . . , nk} who co-own an item — i.e., there is one uploader ∈ N who uploads the item to social media and the rest in N are users affected by the item; and their individual (possibly conflicting) privacy policies Pn1 , . . . , Pnk for that item; how can the negotiating users agree on with whom, from the set of the target users T = {t1, . . . , tm}, the item should be shared? This problem can be decomposed into: 1) Given the set of individual privacy policies Pn1 , . . . , Pnk of each negotiating user for the item, how can we identify if at least two policies have contradictory decisions — or conflicts — about whether or not granting target users T access to the item. 2) If conflicts are detected, how can we propose a solution to the conflicts found that respects as much as possible the preferences of negotiating users N.

IV. Proposed System

In this paper, we present the first computational mechanism for social media that, given the individual privacy preferences of each user involved in an item, is able to find and resolve conflicts by applying a different conflict resolution method based on the concessions users' may be willing to make in different situations.

The mediator inspects the individual privacy policies of all users for the item and flags all the conflicts found. Basically, it looks at whether individual privacy policies suggest contradictory access control decisions for the same target user. If conflicts are found the item is not shared preventively.

The mediator proposes a solution for each conflict found. To this aim, the mediator estimates how willing each negotiating user may be to concede by considering: her individual privacy preferences, how sensitive the particular item is for her, and the relative importance of the conflicting target users for her.

Advantages:
The use of a mediator that detects conflicts and suggests a possible solution to them. Works as an interface to the privacy controls of the underlying Social Media infrastructure. We also present a user study comparing our computational mechanism of conflict resolution and other previous approaches to what users would do themselves manually in a number of situations. The results obtained suggest our proposed mechanism significantly outperformed other previously proposed approaches in terms of the number of times it matched participants' behavior in the study.

V. Related Work

Until now, very few researchers considered the problem of resolving conflicts in multi-party privacy management for Social Media. Wishart et al. proposed a method to define privacy policies collaboratively. In their approach all of the parties involved can define strong and weak privacy preferences. However, this approach does not involve any automated method to solve conflicts, only some suggestions that the users might want to consider when they try to solve the conflicts manually. The work described based on an incentive mechanism where users are rewarded with a quantity of numeraire each time they share information or acknowledge the presence of other users (called co-owners) who are affected by the same item. When there are con- flicts among co-owners' policies, users can spend their numeraire bidding for the policy that is best for them. Then, the use of the Clark Tax mechanism is suggested to obtain the highest bid.

As stated , users may have difficulties to comprehend the mechanism and specify appropriate bid values in auctions. Furthermore, users that earned much numeraire in the past will have more numeraire to spend it at will, potentially leading to unilateral decisions. Users must manually define for each item: the privacy settings for the item, their trust to the other users, the sensitivity of the item, and how much privacy risk they would like to take.

These parameters are used to calculate what the authors call privacy risk and sharing loss on segments - they define segments as the set of conflicting target users among a set of negotiating users. Then, based on these measures all of the conflicting target users in each segment are assigned the same action. That is, all of the conflicts that a set of negotiating users have would be solved either by granting or denying access. Clearly, not considering that each individual conflict can have a different solution leads to outcomes that are far from what the users would be willing to accept. Moreover, due to how the privacy risk and sharing loss metrics are defined, solutions are likely to be the actions preferred by the majority of negotiating users, which can be many times far from the actual behaviour of users.

There are also related approaches based on voting in the literature. In these cases, a third party collects the decision to be taken (granting/denying) for a particular friend from each party. Then, the authors propose to aggregate a final decision based on one of the voting rules already been described— i.e., uploader overwrites (UO), majority voting (MV), and veto voting (VV). These approaches are static, in the sense that they always aggregate individual votes in the same way by following the same voting rule. Thus, these approaches are unable to adapt to different situations that can motivate different concessions by the negotiating users, which makes these approaches unable to match the actual behaviour of users many times. Only, the authors consider that a different voting rule could be applied depending on the situation.

However, it is the user who uploads/posts the item the one who chooses manually which one of the voting rules (UO, MV, VV) to apply for each item. The main problem with this — apart from having to specify the voting rule manually for every item — is that the choice of the voting rule to be applied is unilateral. That is, the user that uploads the item decides the rule to apply without considering the rest of the negotiating users' preferences, which becomes a unilateral decision on a multi-party setting. Moreover, it might actually be quite difficult for the user that uploads the item to anticipate which voting rule would produce the best result without knowing the preferences of the other users.

Finally, the problem of negotiating a solution to multiparty conflicts, has also been recently analysed from a game-theoretic point of view. These proposals provide an elegant analytic framework proposing negotiation protocols to study the problem and the solutions that can be obtained using well-known gametheoretic solution concepts such as the Nash equilibrium.

However, as shown, these proposals may not always work well in practice, as they do not capture the social idiosyncrasies considered by users in the real life when they face multi-party privacy conflicts, and users' behaviour is far from perfectly rational as assumed in these game-theoretic approaches.

VI. MODULES DESCRIPTION

Estimating the Willingness to change an action:
In order to find a solution to the conflict that can be acceptable by all negotiating users, it is key to account for how important is for each negotiating user to grant/deny access to the conflicting target user. In particular, the mediator estimates how willing a user would be to change the action (granting/denying) she prefers for a target agent in order to solve the conflict based on two main factors: the sensitivity of the item and the relative importance of the conflicting target user.

Estimating Item Sensitivity:
If a user feels that an item is very sensitive for her4, she will be less willing to accept sharing it than if the item is not sensitive for her. One way of eliciting item sensitivity would be to ask the user directly, but this would increase the burden on the user. Instead, the mediator estimates how sensitive an item is for a user based on how strict is her individual privacy policy for the item so that the stricter the privacy policy for the item the more sensitive it will be. Intuitively, the lower the number of friends granted access, the stricter the privacy policy, hence, the more sensitive the item is.

Moreover, not all friends are the same; i.e., users may feel closer to some friends than others and friends may be in different groups representing different social contexts. Thus, both the group and the strength of each relationship are considered when estimating the strictness of privacy policies and, therefore, the sensitivity of items.

Estimating the relative importance of the conflict:
Now the focus is on the particular conflicting target user i.e., the target user for which different negotiating users prefer a different action (denying/granting access to the item). The mediator estimates how important a conflicting target user is for a negotiating user by considering both tie strength with the conflicting target user and the group (relationship type) the conflicting target user belongs to which are known to play a crucial role for privacy management. For instance, Alice may decide she does not want to share a party photo with her mother, who has a very close relationship to Alice (i.e., tie strength between Alice and her mother is high). This signals that not sharing the photo with her mother is very important to Alice, e.g., teens are known to hide from their parents in social media. Another example would be a photo in which Alice is depicted together with some friends with a view to a monument that she wants to share with all her friends.

Estimating Willingness:
Finally, the mediator estimates the willingness to change the preferred action (granting/denying) for a conflicting target user accounting for both the sensitivity of the item and the relative importance of the conflicting target user as detailed above. If both sensitivity and relative importance are the highest possible, then the willingness to change should be minimal. On the contrary, if both sensitivity and relative importance are the lowest possible, then the willingness to change should be maximal. Thus, we define willingness as a distance (in a 2-dimensional space) between the values of both item sensitivity and relative importance and the maximum possible values for both.

Modeling Concessions:
As suggested by existing research negotiations about privacy in social media are collaborative most of the time. That is, users would consider others' preferences when deciding to whom they share, so users may be willing to concede and change their initial most preferred option. Being able to model the situations in which these concessions happen is of crucial importance to propose the best solution to the conflicts found — one that would be acceptable by all the users involved. To this aim, the mediator models users' decision-making processes during negotiations based on the willingness to change an action (defined above) as well as on findings about manual negotiations in this domain, like the ones described.

VII. DISCUSSION

The results of the user study suggest that our mechanism was able to match participants concession behaviour significantly more often than other existing approaches. The results also showed the benefits that an adaptive mechanism like the one we presented in this paper can provide with respect to more static ways of aggregating users individual privacy preferences, which are unable to adapt to different situations and were far from what the users did themselves. Importantly, our mechanism is agnostic to and independent from how a user interface communicates the suggested solutions to users and gets feedback from them. First, privacy visualisation tools already proved to be highly usable for social media could be used to show and/or modify the suggested solution, such as Audience View, PViz, or the Expandable Grid. Second, users could define a default response to the solutions suggested, e.g., always accept the suggested solution without asking me9 , which, as shown in the evaluation, would actually match user behaviour very accurately. Other suitable defaults could be applied based on approaches like, or users' responses could be (semi-)automated based on the concession rules instantiated in each situation, using any of the machine-learning approaches shown to work very well in social media privacy settings.

We considered the individual privacy preferences of each individual involved in an item, sensitivity of the item and the relative importance of the target to determine a user's willingness to concede when a multiparty privacy conflict arises. Although accuracy results presented in the previous section are encouraging, this does not mean that there are no other factors that play a role to determine concessions. For instance, in ecommerce domains the strength of relationships among negotiators themselves is also

known to influence to what extent negotiators are willing to concede during a negotiation.

Future research should look into how other factors could help further increase the accuracy of the mechanism presented here. Finally, we focused on detecting and resolving conflicts once we know the parties that co-own an item and have their individual privacy policies for the item. However, we are not proposing a method to automatically detect which items are co-owned and by whom they are co-owned. This is a different problem that is out of the scope of this paper. For example, Facebook researchers developed a face recognition method that correctly identifies Facebook users in 97.35% of the times. Also, it could be the case that a person does not have an account in a given social media. In that case, her face could be preventively blurred. Blurring faces may seriously diminish the utility of sharing information in social media, but it could also be a good alternative if no agreement is reached between negotiators to ensure an individual (not collective) privacy baseline is achieved.

VIII. Conclusion

In this paper, we present the first mechanism for detecting and resolving privacy conflicts in Social Media that is based on current empirical evidence about privacy negotiations and disclosure driving factors in Social Media and is able to adapt the conflict resolution strategy based on the particular situation. In a nutshell, the mediator firstly inspects the individual privacy policies of all users involved looking for possible conflicts. If conflicts are found, the mediator proposes a solution for each conflict according to a set of concession rules that model how users would actually negotiate in this domain.

We conducted a user study comparing our mechanism to what users would do themselves in a number of situations. The results obtained suggest that our mechanism was able to match participants' concession behavior significantly more often than other existing approaches. This has the potential to reduce the amount of manual user interventions to achieve a satisfactory solution for all parties involved in multi-party privacy conflicts. Moreover, the study also showed the benefits that an adaptive mechanism like the one we presented in this paper can provide with respect to more static ways of aggregating users' individual privacy preferences, which are unable to adapt to different situations and were far from what the users did themselves.

The research presented in this paper is a stepping stone towards more automated resolution of conflicts in multi-party privacy management for Social Media.

IX. Future Work

We plan to continue researching on what makes users concede or not when solving conflicts in this domain. In particular, we are also interested in exploring if there are other factors that could also play a role in this, like for instance if concessions may be influenced by previous negotiations with the same negotiating users or the relationships between negotiators themselves.

X. REFERENCES

[1]. Internet.org, "A focus on efficiency," http://internet.org/efficiencypaper,Retr.09/2014 .

[2]. K. Thomas, C. Grier, and D. M. Nicol, "unfriendly: Multi-party privacy risks in social networks," in Privacy Enhancing Technologies. Springer, 2010, pp. 236-252.

[3]. A. Lampinen, V. Lehtinen, A. Lehmuskallio, and S. Tamminen, "We're in it together: interpersonal management of disclosure in social network services," in Proc. CHI. ACM, 2011, pp. 3217-3226.

[4]. P.Wisniewski, H. Lipford, and D.Wilson, "Fighting for my space: Coping mechanisms for sns boundary regulation," in Proc. CHI.ACM, 2012, pp. 609-618.

[5]. A. Besmer and H. Richter Lipford, "Moving beyond untagging: photo privacy in a tagged world," in ACM CHI, 2010, pp. 1563-1572.

[6]. Facebook NewsRoom, "One billion- key metrics," http://newsroom.fb.com/download-media/4227,Retr.26/06/2013.

[7]. J. M. Such, A. Espinosa, and A. Garcıa-Fornes, "A survey of privacy in multi-agent systems," The Knowledge Engineering Review, vol. 29, no. 03, pp. 314-344, 2014.