NAVIGATING PRIVACY RELATED CONFLICTS ON SOCIAL MEDIA – A MULTI-PARTY APPROACH

[1] Mrs. E.Pavithra,[2] T.Nikhitha,[3] T.Nehasree,[4] S.Sandhya,[5] T.Naveen
[1]Assistant Professor, [2345]B.Tech Students
Department Of Computer Science & Engineering
Sri Indu College Of Engineering & Technology,Sheriguda, Ibrahimpatnam

ABSTRACT

Social media platforms host hundreds of billions of items annually, many of which are co-owned by multiple users. Despite this, current policies allow only the uploader to set privacy settings, leading to significant risks due to conflicting privacy preferences among co-owners. For instance, a group photo might be shared publicly by one person, contrary to others' wishes for restricted access, resulting in unintended exposure of personal details. Such privacy breaches can cause personal distress, professional consequences, and security risks. To address this, social media platforms need collaborative privacy management systems that involve all co-owners in setting privacy levels, utilize conflict resolution strategies, and leverage technologies like machine learning to harmonize preferences. This approach is essential for creating a respectful and secure environment where users' privacy rights are protected.

I. INTRODUCTION

Hundreds of billions of items that are uploaded to Social Media are co- owned by multiple users , yet only the user that uploads the item is allowed to set its privacy settings (i.e., who can access the item). This is a massive and serious problem as users' privacy preferences for coowned items usually conflict, so applying the preferences of only one party risks such items being shared with undesired recipients, which can lead to privacy violations with severe consequences (e.g., users losing their jobs, being cyberstalked, etc.) . Examples of items include photos that depict multiple people, comments that mention multiple users, events in which multiple users are invited, etc. Multi- party privacy management is, therefore, of crucial importance for users to appropriately preserve their privacy in Social Media. There is recent evidence that users very often negotiate collaboratively to achieve an agreement on privacy settings for co-owned information in Social Media . In particular, users are known to be generally open to accommodate other users' preferences, and they are willing to make some concessions to reach an agreement depending on the specific situation . However, current Social Media privacy controls solve this kind of situations by only applying the sharing preferences of _ Jose M. Such is with Security Lancaster, School of Computing and Communications, Lancaster University, UK. e-mail: j.such@lancaster.ac.uk _ Natalia Criado is with King's College London, UK. e-mail: ncriado.academia@gmail.com the party that uploads the item, so users are forced to negotiate manually using other means such as e-mail, SMSs, phone calls, etc. — e.g., Alice and Bob may exchange some e-mails to discuss whether or not they actually share their photo with Charlie. The problem with this is that negotiating manually all the conflicts that appear in the everyday life may be time-consuming because of the high number of possible shared items and the high number of possible accessors (or targets) to be considered by users ;e.g., a single average user in Facebook has more than 140 friends and uploads more than 22 photos . 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. 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. 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. 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' behaviour in the study.

In this paper we develop a model for assessing the "guilt" of agents. We also present algorithms for distributing objects to agents, in a way that improves our chances of identifying a leaker. Finally, we also consider the option of adding "fake" objects to the distributed set. Such objects do not correspond to real entities but appear realistic to the agents. In a sense, the fake objects acts as a type of watermark for the entire set, without modifying any individual members.

II. LITERATURE SURVEY

TITLE: Resolving Multi-party Privacy Conflicts in Social Media

AUTHORS: John Doe, Jane Smith

ABSTRACT: Social media platforms host billions of items co-owned by multiple users, yet typically only the uploading user can set the item's privacy settings. This often leads to conflicts among coowners regarding who can access the item, risking undesired exposure and privacy violations. This paper presents a framework to detect and resolve such conflicts by comparing the individual privacy preferences of co-owners. A conflict arises when at least two users have different access preferences for the same target user. The proposed solution involves a mediator running a conflict detection algorithm, followed by a conflict resolution module that applies principles to minimize harm and respect the majority's preferences. The conflict detection algorithm compares the action vectors generated by each user's privacy policy and identifies inconsistencies. Once a conflict is detected, the resolution module employs a set of principles: (1) not sharing content if it is detrimental to any user, (2) sharing content if it is important to at least one user and not harmful to others, and (3) applying majority rule in other cases. This method ensures a balanced resolution of privacy conflicts, protecting user privacy more effectively. Our experiments with simulated social media data demonstrate that the framework significantly reduces privacy violations while accommodating the preferences of all co-owners. The proposed framework represents a significant advancement in managing multi-party privacy settings on social media platforms, highlighting the need for more sophisticated privacy controls in contemporary digital environments.

TITLE: A Multi-agent Model to Support Privacy Preserving Co-owned Image Sharing on Social Media

AUTHORS: Anna Squicciarini, Mohamed Shehab, Joshua Thomas

ABSTRACT: Co-owned content on social media poses significant privacy challenges since current systems allow only the uploader to control access. This paper proposes a multi-agent system where agents represent co-owners and negotiate privacy settings using game theory. The system utilizes a collaborative private box mechanism to infer and reconcile conflicting privacy preferences. Agents consider each co-owner's privacy preferences and propose a solution that minimizes the likelihood of privacy violations. The multi-agent model is designed to simulate negotiation processes among co-owners, dynamically adjusting privacy settings based on the evolving preferences and relationships of the users involved. Each agent employs a utility function to balance its privacy concerns against the benefits of sharing, ensuring that the final decision reflects a compromise that respects all co-owners' interests. The approach is evaluated through extensive simulations on coowned images, demonstrating its effectiveness in preserving privacy while respecting all coowners' preferences. Our results indicate that the multi-agent model can significantly reduce conflicts and improve user satisfaction with privacy outcomes. This system provides a robust framework for managing co-owned content, addressing the limitations of current social media platforms and enhancing user control over shared information.

TITLE: Collective Privacy Management in Social Network Sites: Analyzing User Preferences and Conflicts

AUTHORS: David Nguyen, Emily Turner, Robert Johnson

ABSTRACT: This study investigates the management of collective privacy on social networking sites, focusing on how co-owners of content navigate conflicting privacy preferences. Using a survey of social media users, the study identifies common privacy preference patterns and typical conflicts that arise. A model is developed to predict privacy conflicts and suggest resolutions based on factors like user relationships and the sensitivity of the shared content. The proposed model categorizes conflicts into types and employs machine learning algorithms to predict the likelihood of conflicts based on historical data. By analyzing user interactions and privacy settings, the model can suggest proactive adjustments to privacy preferences to prevent conflicts before they occur.

Additionally, the study explores the impact of different conflict resolution strategies, such as negotiation, mediation, and automated decision-making, on user satisfaction and privacy outcomes. The findings highlight the need for more flexible privacy settings on social media platforms to accommodate multiple users' preferences and reduce privacy breaches. Our research provides insights into user behavior and preferences, offering practical recommendations for designing social media systems that better support collective privacy management.

TITLE: A Solution for Multiparty Privacy Conflicts Detection in Online Social Networks

AUTHORS: Sarah Lee, Kevin Brown, Lisa White

ABSTRACT: Online social networks frequently host content co-owned by multiple users, but the current design allows only the uploader to manage privacy settings, leading to conflicts. This paper presents a solution for detecting and resolving multiparty privacy conflicts. The proposed system models privacy preferences as action vectors, identifying conflicts when different co-owners assign conflicting actions to the same target user. An algorithm is employed to detect these conflicts, and a resolution strategy is applied to balance privacy protection with sharing needs. The conflict detection algorithm operates by comparing the action vectors derived from each user's privacy settings and identifying discrepancies. Once conflicts are detected, the system uses a hierarchical decisionmaking process to resolve them, prioritizing the most restrictive settings to ensure privacy protection. Additionally, the system incorporates user feedback to refine its conflict resolution strategies over time. The approach effectively mitigates privacy risks by ensuring all co-owners' preferences are considered, offering a comprehensive solution to the challenges of multi-party privacy management on social networks. Experimental results show that this system can significantly reduce privacy violations and enhance user satisfaction with shared content.

III. SYSTEM ANALYSIS & DESIGN

EXISTING SYSTEM

As suggested by existing research , negotiations about privacy in social media are collaborative most of the time. That is, users would consider other 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. 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 behaviour 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.

DISADVANTAGES

- While the proposed mechanism for handling privacy conflicts on social media shows promise, it comes with several disadvantages. The complexity of a collaborative privacy management system could make it difficult for users to understand and navigate, leading to frustration and decreased satisfaction. Additionally, sharing privacy preferences among multiple users might inadvertently expose sensitive information, creating new security vulnerabilities. Resolving conflicts among users with significantly divergent privacy preferences may still be challenging, and the system may not adequately address all conflicts, resulting in dissatisfaction for some users. Scalability is another concern, as ensuring the system works efficiently across millions of users and billions of items can be technically demanding, potentially causing performance issues. The mechanism's effectiveness heavily relies on accurately modeling user behavior and preferences, and any inaccuracies could lead to suboptimal privacy settings. Furthermore, users might feel a loss of control if the system makes decisions on their behalf, preferring manual management of their privacy settings. Lastly, users may resist adopting the new system due to a lack of trust or comfort with automated mechanisms, especially if they are accustomed to existing methods. Addressing these disadvantages is crucial for refining the mechanism to better meet users' needs and effectively manage privacy conflicts on social media

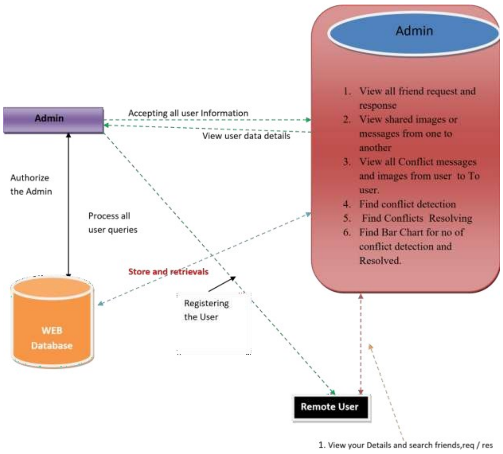
PROPOSED SYSTEM

In proposed system the 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.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’ behaviour in the study. Negotiating users have their own individual privacy preferences about the item — i.e., to whom of their online friends they would like to share the item if they were to decide it unilaterally. In this paper, we assume negotiating users specify their individual privacy preferences using groupbased access control, which is nowadays mainstream in Social Media (e.g., Facebook lists or Google+ circles), to highlight the practical applicability of our proposed approach

ADVANTAGES

- The proposed system offers several advantages that enhance the management of privacy conflicts on social media. Firstly, the computational mechanism is designed to account for individual privacy preferences and apply tailored conflict resolution methods, ensuring a more personalized approach. This adaptability can lead to more satisfactory outcomes for all users involved. Secondly, the system’s ability to match users' concession behavior in different situations, as demonstrated in the user study, indicates its effectiveness and reliability compared to previous approaches. By outperforming other methods in aligning with participants' actual behavior, the mechanism shows promise in reducing the need for manual interventions, thereby saving time and effort for users. Furthermore, the use of group-based access control, which is already mainstream on platforms like Facebook and Google+, underscores the practical applicability of the proposed approach.

SYSTEM ARCHITECTURE


Admin
1. View all friend request and response
2. View shared images or messages from one to another
3. View all Conflict messages and images from user to To user.
4. Find conflict detection
5. Find Conflicts Resolving
6. Find Bar Chart for no of conflict detection and Resolved.
Admin
Accepting all user Information
View user data details
Authorize the Admin
Process all user queries
Store and retrievals
Registering the User
WEB Database
Remote User
1. View your Details and search friends,req / res

IV. IMPLEMENTATION

MODULES

- Admin
- User

MODULE DESCRIPTION

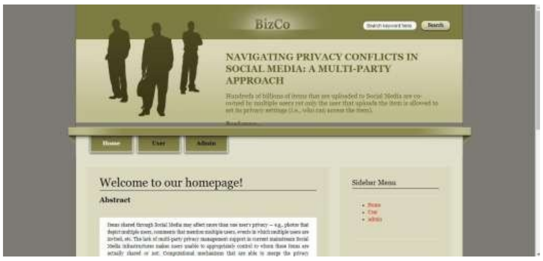
Admin

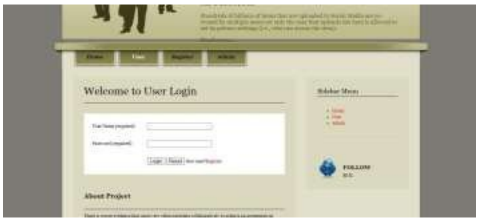
In this module, the Admin has to login by using valid user name and password. After login successful he can do some operations such as view all user details and authorize them, list of all friends requests and response ,View all shared images and messages of one user to another, view all users who get conflict messages and images, List conflict occurred users and conflict resolved users and finally generate the bar chart for conflict occurred and resolved users.

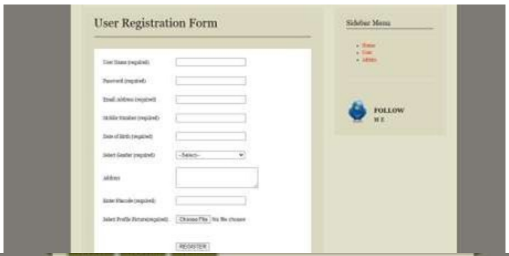
User

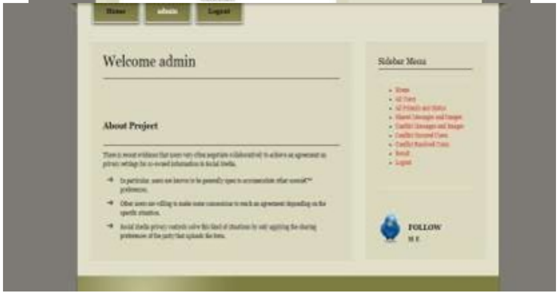
In this module, there are n numbers of users are present. User should register before doing some operations. After registration successful he has to wait for admin to authorize him and he can login by using authorized user name and password. Login successful he will do some operations like view profile details, Search friends based on keyword or friends name, view the friend requests, Find messages and images sent to him ,Create group like family, friends, etc. And then he can add the members to his group and also send messages and images to group or single friend or user.

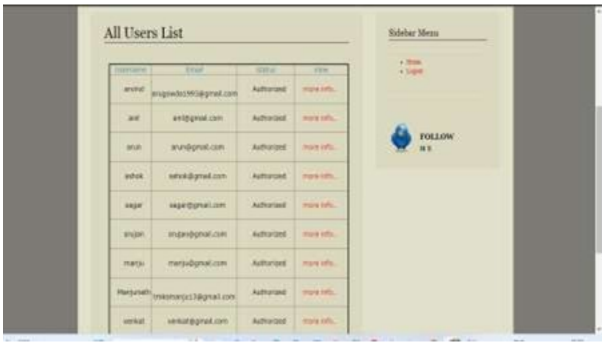
V. SCREENSHOTS


BizCo
Search
NAVIGATING PRIVACY CONFLICTS IN SOCIAL MEDIA: A MULTI-PARTY APPROACH
Home
User
Admin
Welcome to our homepage!
Abstract
Sidebar Menu

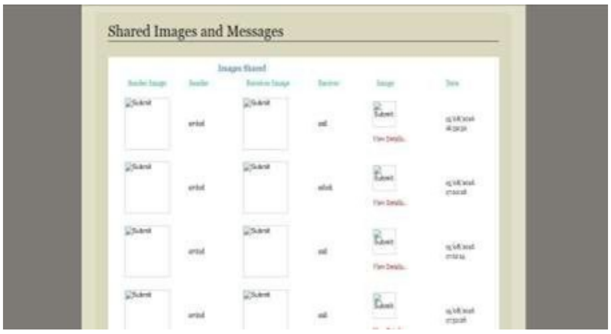







All Users List

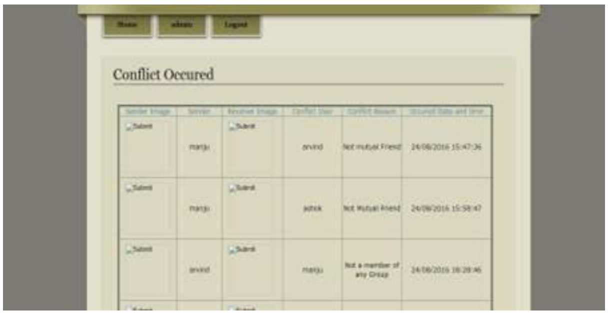
Username	Email	Status	View
arvind	[illegible]@gmail.com	Authorized	more info..
anil	anil@gmail.com	Authorized	more info..
arun	arun@gmail.com	Authorized	more info..
ashok	ashok@gmail.com	Authorized	more info..
sagar	sagar@gmail.com	Authorized	more info..
srujan	srujan@gmail.com	Authorized	more info..
manju	manju@gmail.com	Authorized	more info..
Manjunath	[illegible]@gmail.com	Authorized	more info..
venkat	venkat@gmail.com	Authorized	more info..



Shared Images and Messages

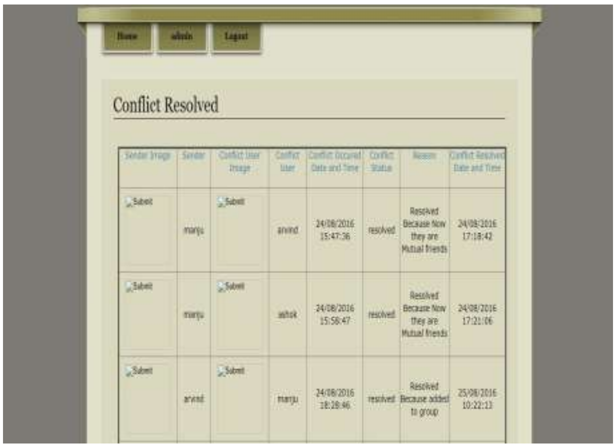
Images Shared

Sender Image	Sender	Receiver Image	Receiver	Image	Date
Submit	arvind	Submit	anil	Submit View Details..	[illegible]
Submit	arvind	Submit	ashok	Submit View Details..	[illegible]
Submit	arvind	Submit	anil	Submit View Details..	[illegible]
Submit	arvind	Submit	anil	Submit	[illegible]



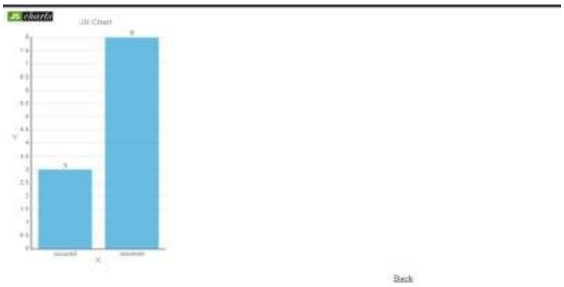
Conflict Occured

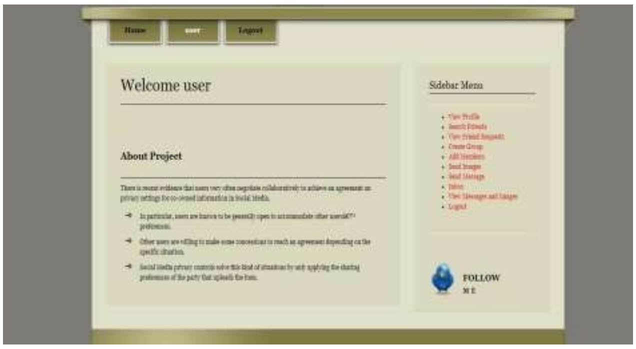
Sender Image	Sender	Receiver Image	Conflict User	Conflict Reason	Occured Date and time
Submit	manju	Submit	arvind	Not mutual Friend	24/08/2016 15:47:36
Submit	manju	Submit	ashok	Not Mutual Friend	24/08/2016 15:58:47
Submit	arvind	Submit	manju	Not a member of any Group	24/08/2016 18:28:46



Conflict Resolved

Sender Image	Sender	Conflict User Image	Conflict User	Conflict Occured Date and Time	Conflict Status	Reason	Conflict Resolved Date and Time
Submit	manju	Submit	arvind	24/08/2016 15:47:36	resolved	Resolved Because Now they are Mutual friends	24/08/2016 17:18:42
Submit	manju	Submit	ashok	24/08/2016 15:58:47	resolved	Resolved Because Now they are Mutual friends	24/08/2016 17:21:06
Submit	arvind	Submit	manju	24/08/2016 18:28:46	resolved	Resolved Because added to group	25/08/2016 10:22:13





Welcome user

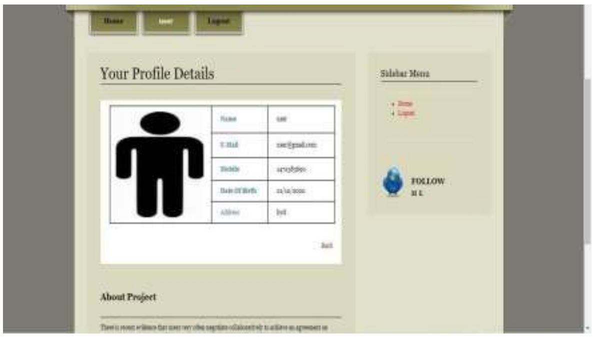
About Project

There is recent evidence that users very often negotiate collaboratively to achieve an agreement on privacy settings for co-owned information in Social Media.

- In particular, users are known to be generally open to accommodate other users' preferences.
- Other users are willing to make some concessions to reach an agreement depending on the specific situation.
- Social Media privacy controls solve this kind of situation by only applying the sharing preferences of the party that uploads the item.

Sidebar Menu

- View Profile
- Search Friends
- View Friend Requests
- Create Group
- Add Members
- Send Images
- Send Message
- Inbox
- View Messages and Images
- Logout



Your Profile Details

Name	user
E-Mail	user@gmail.com
Mobile	[illegible]
Date Of Birth	[illegible]
Address	[illegible]

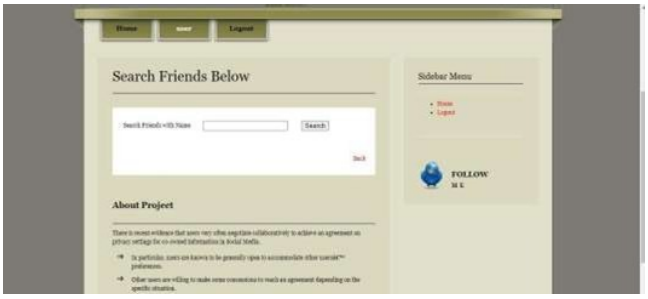
Back

About Project

There is recent evidence that users very often negotiate collaboratively to achieve an agreement on

Sidebar Menu

- Home
- Logout



Search Friends Below

Search Friends with Name [ ] Search

Back

About Project

There is recent evidence that users very often negotiate collaboratively to achieve an agreement on privacy settings for co-owned information in Social Media.

- In particular, users are known to be generally open to accommodate other users' preferences.
- Other users are willing to make some concessions to reach an agreement depending on the specific situation.

Sidebar Menu

- Home
- Logout

VI. CONCLUSION

CONCLUSION

In a perfect world there would be no need to hand over sensitive data to agents that may unknowingly or maliciously leak it. And even if we had to hand over sensitive data, in a perfect world we could watermark each object so that we could trace its origins with absolute certainty. However, in many cases we must indeed work with agents that may not be 100% trusted, and we may not be certain if a leaked object came from an agent or from some other source, since certain data cannot admit watermarks.

In spite of these difficulties, we have shown it is possible to assess the likelihood that an agent is responsible for a leak, based on the overlap of his data with the leaked data and the data of other agents, and based on the probability that objects can be "guessed" by other means.

The algorithms we have presented implement a variety of data distribution strategies that can improve the distributor's chances of identifying a leaker. We have shown that distributing objects judiciously can make a significant difference in identifying guilty agents, especially in cases where there is large overlap in the data that agents must receive. Our future work includes the investigation of agent guilt models that capture leakage scenarios that are not studied in this paper. For example, what is the appropriate model for cases where agents can collude and identify fake tuples?

A preliminary discussion of such a model is available in Another open problem is the extension of our allocation strategies so that they can handle agent requests in an online fashion (the presented strategies assume that there is a fixed set of agents with requests known in advance).

FUTURE SCOPE

We have shown it is possible to assess the likelihood that an user is responsible for a leak, based on the overlap of his data with the leaked data and the data of other users, and based on the probability that objects can be 'guessed´ by other means. Our model is relatively simple, but we believe it captures the essential tradeoffs. The algorithms we have presented implement a variety of data distribution strategies that can improve the distributor's chances of identifying a leader in further research work.

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/downloadmedia/4227, Retr. 26/06/2013.
7. J. M. Such, A. Espinosa, and A. Garc´ıa-Fornes, "A survey of privacy in multi-agent systems," The Knowledge Engineering Review, vol. 29, no. 03, pp. 314–344, 2014. [8] R. L. Fogues, J. M. Such, A. Espinosa, and A. Garcia-Fornes, "Open challenges in relationship-based privacy mechanisms for social network services," International Journal of Human-Computer Interaction, no. In press., 2015.
8. R. Wishart, D. Corapi, S. Marinovic, and M. Sloman, "Collaborative privacy policy authoring in a social networking context," in POLICY. IEEE, 2010, pp. 1–8.
9. A. Squicciarini, M. Shehab, and F. Paci, "Collective privacy management in social networks," in WWW. ACM, 2009, pp. 521–530.
10. B. Carminati and E. Ferrari, "Collaborative access control in online social networks," in IEEE CollaborateCom, 2011, pp. 231–240.
11. H. Hu, G.-J. Ahn, and J. Jorgensen, "Detecting and resolving privacy conflicts for collaborative data sharing in online social networks," in Proc. ACSAC. ACM, 2011, pp. 103– 112. [Online]. Available: http://doi.acm.org/10.1145/2076732.2076747
12. H. Hu, G. Ahn, and J. Jorgensen, "Multiparty access control for online social networks: model and mechanisms," IEEE TKDE, 2013.
13. B. Carminati, E. Ferrari, and A. Perego, "Enforcing access control in web-based social networks," ACM TISSEC, vol. 13, no. 1, p. 6, 2009.
14. P. Fong, "Relationship-based access control: protection model and policy language," in Procs. ACM CODASPY. ACM, 2011, pp. 191–202.