Enabling Co-owned Image Privacy on Social Media via Agent Negotiation

Farzad N. Motlagh
Hasso-Plattner-Institute for Digital Engineering,
University of Potsdam
Potsdam, Germany
farzad.motlagh@hpi.de

Anne V.D.M. Kayem
Hasso-Plattner-Institute for Digital Engineering,
University of Potsdam
Potsdam, Germany
anne.kayem@hpi.de

Nikolai J. Podlesny
Hasso-Plattner-Institute for Digital Engineering,
University of Potsdam
Potsdam, Germany
nikolai.podlesny@hpi.de

Christoph Meinel
Hasso-Plattner-Institute for Digital Engineering,
University of Potsdam
Potsdam, Germany
meinel@hpi.de

ABSTRACT

Social media has become a popular communication platform on which shared content such as images form a large part of the communicated data. Yet, shared images can reveal sensitive information in the sense that the data after its publication remains accessible. Existing studies provide mechanisms to modify co-owned images for user privacy but require that every user involved be online in order to reach an agreement. In cases where users are offline at the time when the image is posted, no privacy agreement can be reached. Having a method of reaching a privacy agreement even when some of the users in the co-owned image are offline is useful in enforcing individual privacy settings vis-a-vis the co-owned image. In this paper, we present a multi-agent negotiation model that enforces individual privacy settings with respect to co-owned images even when the users are offline. Our multi-agent model includes three components, namely a coordinator agent, predictor agent, and filtering algorithm. The coordinator agent collects users' opinions vis-a-vis a co-owned image to form an image that expresses the opinions of the involved users. The predictor agent supports the expression of offline user opinions, while the filtering algorithm removes privacy-violating information with respect to recent user opinions. Results from our proof-of-concept implementation indicate that improved efficiency in terms of privacy decisions can be achieved by employing agents to support offline user decisions regarding shared content.

CCS CONCEPTS

• **Computer systems organization** → **Embedded systems**; *Redundancy*; Robotics; • **Networks** → Network reliability.

iiWAS2021, November 29-December 1, 2021, Linz, Austria

ACM ISBN 978-1-4503-9556-4/21/11.
https://doi.org/10.1145/3487664.3487685

KEYWORDS

Online social network, privacy, agent, collaboration, negotiation

ACM Reference Format:
Farzad N. Motlagh, Anne V.D.M. Kayem, Nikolai J. Podlesny, and Christoph Meinel. 2021. Enabling Co-owned Image Privacy on Social Media via Agent Negotiation. In *The 23rd International Conference on Information Integration and Web Intelligence (iiWAS2021), November 29-December 1, 2021, Linz, Austria.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3487664.3487685

1 INTRODUCTION

Online social networks allow users to upload and share large volumes of content [3]. A key benefit of Online Social Networks (OSNs) is that they make people feel closer by enabling shared multimedia content. Images and videos, for instance, from a large bulk of the shared content [12].

The nature of shared co-owned image, however, increases the risk of sensitive information exposure. This is in the sense that uploaded images on OSNs tend to contain information on multiple individuals (co-owners). Sharing such co-owned images without the explicit permission of the co-owners can violate users' privacy settings.

An example scenario arises in the case of a co-owned image that is posted to an OSN. The posted image includes three users: Alice (content uploader), Bob (co-owner), and Carol (close friend). In this case, a content uploader is a user who intends to post an image on an OSN like Instagram. This user can be either the owner or a user who appears in the image. A co-owner is a user or group of users who have co-ownership on a shared image. Furthermore, a user called a close friend that has permission to view a shared co-owned image.

The image is a photo that Alice took at Bob's graduation party to share with her friends on OSNs. However, Bob considered his graduation to be kept secret. Furthermore, Carol has two positions in this scenario: first, she is a friend of Alice and can observe all the contents that Alice posts on the OSN; and second, Carol is Bob's boss [2]. In this case, Alice decides to post the image on her OSN without tagging Bob as an image co-owner. By checking the image posted by Alice, Carol finds out that the image was taken at Bob's graduation party. Therefore, Alice inadvertently

reveals Bob's private information to Carol by posting the co-owned image without explicitly obtaining Bob's permission. In this regard, having a method of sharing co-owned content or group decision-making [1] in a privacy-preserving manner is an important step in protecting users' privacy vis-a-vis co-owned content on OSNs.

In group decision-making, a group of users (or experts) contribute their opinions to reach a consensus on a joint privacy decision. This joint privacy decision is then used as an optional solution with respect to the users' privacy constraints related to the shared co-owned content.

In the standard approach to posting shared content (images), all co-owners must be physically online and actively agree to having the content posted. This poses a problem when the users involved (co-owners) are either offline or fail to provide a response. In order to address this problem, in this paper, we propose an agent-based negotiation model to protect users' private information even when the users concerned are offline. Our proposed model is composed of three components, namely a coordinator agent, a predictor agent, and a filtering algorithm. When an image is ready to be posted, the coordinator agent, which is associated with the user wanting to post the image, collects opinions submitted by both online users and user agents acting on behalf of offline (or inactive) users. The predictor agent supports the user agents in coming to an opinion that is representative of the affected user's opinion. In order to achieve this, the predictor agent computes opinions based on previous opinions provided by the affected users in similar contexts as well as an averaging mechanism. When there is no opinion history, an opinion is determined based on similar user profiles. Once all the opinions have been collected, the coordinator agent uses the filtering algorithm to blur (remove) all privacy-violating information from the image based on users'/agents' opinions.

The rest of the paper is organized as follows. Section 2 introduces recent approaches on collaborative privacy management. Our proposed solution is presented in Section 3. Empirical results are provided in Section 4, and finally, a concluding statement is offered in Section 5.

2 RELATED WORK

Typically, each user on an OSN has different privacy settings. To avoid conflicts that originate from different privacy interests with respect to shared content, the OSNs must restrict user permissions to online content that they wish to share. This is typically achieved with constraints on users who have the desire to access published data. Work on collaborative privacy-preserving content sharing on OSNs was triggered by Squicciarini et al. [10].

Squicciarini et al. [10] proposed a Clarke-Tax technique that allows users to specify their preferred privacy settings before posting online content. However, this collaborative privacy management approach does not take all users' preferences into account. Wishart et al. [15] address this caveat with a policy permitting content uploaders to specify some shared content policies. Still, their approach does not cover all users' privacy settings since these change dynamically.

To address changing privacy requirements, Hu et al. [8] suggested a simple cost-benefit framework that considered either data sharing loss or privacy risk. Furthermore, Joseph [9] formulated

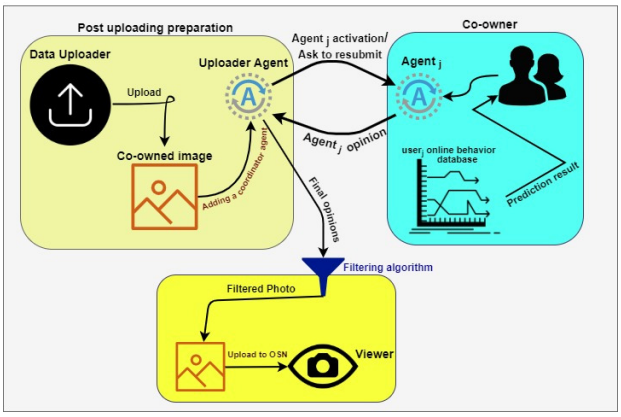

Figure 1: Multi-Agent Privacy Model

a solution to cope with privacy conflicts. The approach proposed by Joseph [9] utilized partitions to identify conflicts in accessor space segments. Multi-party access control was offered by Suvitha [11]. According to Suvitha's [11] approach, a viewer should follow a two-step verification process to access online content. A privacy protection approach considering both unlisted friends and OSN service providers was proposed by Ali et al. [2]. In their approach [2], a cartographic framework was suggested to address the OSN privacy concerns. Ulusoy [13] provided an improved Clarke-Tax method, and Du et al. [4] exploited an evolutionary game model to protect user's privacy.

3 PRIVACY NEGOTIATIONS MULTI-AGENT MODEL

The process of content sharing starts with uploading a co-owned image on an OSN. Co-owners must confirm that the online content can be shared. This is essential in guaranteeing user privacy vis-a-vis shared content. Using general privacy settings does not adequately protect individual user privacy. To protect users' privacy by considering each user's specific interest, we cannot offer, and also apply, general data protection rules for all clients. Therefore, having a model that supports users in customizing their privacy settings and making explicit decisions about the content that would reveal their sensitive data is important.

Our multi-agent model works for privacy by activating a post uploader agent (super agent). The super agent coordinates the operations of the other agents involved in the image posting decision by activating the related agents. Then, this coordinator agent collects opinions either submitted directly by online users or predicted by agents in the case of offline or inactive users.

As shown in Figure 1, a user submits his/her opinion if that client is available (online) on the OSN. Otherwise, the coordinator agent activates the offline users' agent to predict the associated clients' opinions. An $agent_i$ runs a prediction algorithm to explore the users' recent online behaviors. Respecting users' privacy preferences, $agent_i$ returns prediction results to a coordinator agent, which is called uploader agent. Finally, based on the responses which are received from all agents or online users (aggregated feedback), the uploader agent filters the co-owned image of all

privacy-violating data by blurring their faces. We now explain how the privacy preference prediction mechanism works to support the privacy negotiation model.

3.1 Privacy-preference prediction

In our prediction framework, an agent is associated with each user profile to predict the user's privacy preferences in terms of co-owned content. In our approach, each agent$_i$ utilizes equation 1 to predict the user$_i$ behavior.

$$f_i = \frac{\sum_{j=1}^{m} R_j * l_j}{m * z}, \quad 0 \leq l_j \leq 1 \tag{1}$$

where, R$_j$ is the user$_i$ recent opinions about the shared content, l$_j$ is a weight value that indicates the importance of recent opinion$_j$. Accordingly, m is the whole number of recently submitted opinions by user$_i$. Also, z is the maximum value of opinions that a user/agent can submit in the decision process to reach a consensus.

To allow a co-owned image to be shared on an OSN, users/agents have to respect an acceptable range of opinion submissions to determine whether an opinion is strong or not. In standard approaches, users submit their opinions in a predefined range of $t \leq O \leq z$, where t and z are the lowest and highest opinion values that users/agents can submit. Furthermore, the uploader agent checks the received opinions from other agents, and prevents them from submitting an opinion in a special range called indecisive range.

To apply the opinions in the filtering algorithm, the uploader agent rejects transferring the opinions that are distributed in the indecisive range. Applying indecisive range supports agents to predict the behavior of user$_i$ based on users' recent strong opinions about sharing the online content. Strong approvals/disapprovals tend to be more close to the upper/lower bound of z/t. Equation 2 shows the indecisive range. In this case, p and q are lower and upper bounds of the indecisive range, respectively.

$$t < p \leq O \leq q < z \tag{2}$$

To improve privacy protection, the opinions offered by co-owners should not be shared among other users/agents. In this regard, the uploader agent utilizes equation 3 to collect opinions of either users or agents; then, it shares the average value of the collected opinions to other associated agents. These agents need the collected opinions to make better and decisive decisions. Decisive opinions are the opinions that are not located within the indecisive range (see equation 2). Due to privacy concerns, the uploader agent blurs the faces that their opinions are in the indecisive range. It is likely that some agents to be blurred, although they have submitted a positive response about sharing their online image. This is because their opinions are recognized to be within the indecisive range.

$$C = \frac{\sum_{j=1}^{d} f_j + \sum_{i=1}^{h} u_i}{d + h} \tag{3}$$

where f$_j$ is an agent$_j$ opinion about the shared content, which predicts clients' opinions when they are offline. Also, u$_i$ is the online user opinion, and d is the number of agents that are activated; and h is the number of online users; $\sum_{j=1}^{d} f_j$ is the whole agents opinions. Furthermore, $\sum_{i=1}^{h} u_i$ is online users' opinions. The number of opinions received from agents should be equal to or less than the total users since The uploader agent activates agents when their related users are offline.

Figure 2: Blurred faces

In addition to the privacy concerns, using *collected opinions* significantly reduces our algorithm time complexity. Since the uploader agent prevents other agents from communicating with each other directly.

The uploader agent sends C (*collected opinions*) to an agent$_j$ who could not return an acceptable response that is out of the range mentioned in equation 2. Finally, by considering the associated agents' opinions, an agent$_j$ provides its opinion (K$_j$) to send to the uploader agent as follows:

$$K_j = \begin{cases} \frac{(\frac{f_j}{s} + \frac{C}{w})}{2}, & \text{for } C \geq z/2, p \leq f_j \leq q \\ \frac{(|\frac{f_j}{s} - \frac{C}{w}|)}{2}, & \text{for } C < z/2, p \leq f_j \leq q \\ f_j, & \text{for } f_j > q \mid f_j < p \end{cases} \tag{4}$$

By considering $t < \{s, w\} \leq z$, f$_j$ is an agent$_j$ opinion, s and w are weight values that indicate the importance of the target user/agent opinion and co-owners views, respectively. Agent$_j$ submits K$_j$ to the uploader agent. In this way, agent$_j$ predicts the privacy preference of the user$_j$ without having a direct negotiation with other agents.

4 RESULTS

4.1 Experimental setup

The prediction model introduced in this study was implemented on a system with corei3 Intel CPU 2270 MHz, 6GB RAM, and Windows 10 operating system. We implemented our negotiation model using Python version 3 [14].

To evaluate our approach, we used Gallager et al. [5] dataset. The dataset contains images with the following keywords: wedding, bride, gender, and age. In addition, these images contain individuals in different situations, such as sitting or standing on particular surfaces.

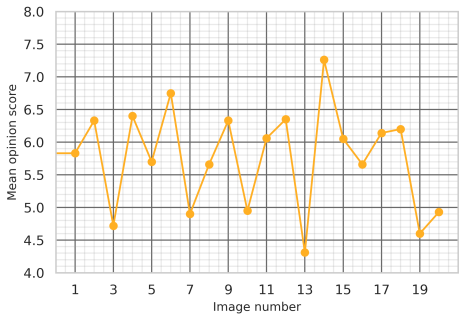

Figure 3: Mean opinion score

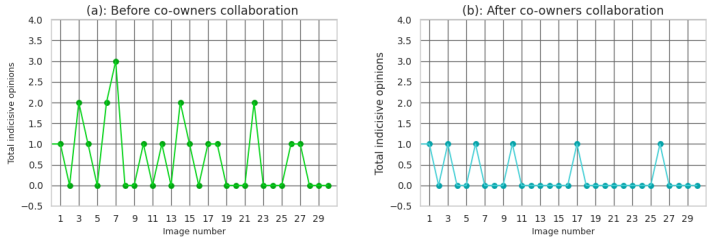

Figure 4: (a) Before co-owner's collaboration (b) After co-owner's collaboration

4.2 Evaluating privacy-preference negotiation model

We utilized Boosted Haarcascade [6] algorithm to detect the co-owners in the shared images. Figure 2 shows the face detection algorithm output. Filtering agent takes face positions and sends them to the uploader agent as well as the associated agents. Furthermore, we applied Gaussian smoothing [7] to blur out the faces belonging to the users/agents that disagreed to grant permission for their private information to be published by the uploader agent.

Figure 3 indicates the mean opinion score submitted by five co-owners. Our negotiation model iterated for 20 steps with different images and the same number of co-owners (five co-owners). According to the results presented in Figure 3, the *collected opinions* submitted by users/agents was 5.74 out of 10.

In addition, in our experimentation, we set indecisive range which is mentioned in equation 2 as $4.5 \leq O \leq 5.5$, z=10, t=0. These numbers are randomly selected values. Figure 4.a presents the number of agents with indecisive responses. The outcome of the algorithm shows 23.8 percent of agents failed to provide an opinion acceptable by the uploader agent. When agents fail to provide an opinion acceptable to the uploader agent, the uploader agent handles this by using the other collected agent and user opinions, from the ones who have provided a valid opinion, to reach a prediction on a possibly acceptable opinion to the failed agents.

Figure 4.b depicts agents' opinions after applying our negotiation scheme coordinated by uploader agent. According to Figure 4.b, 57.15 percent of agents could provide the in range decision in

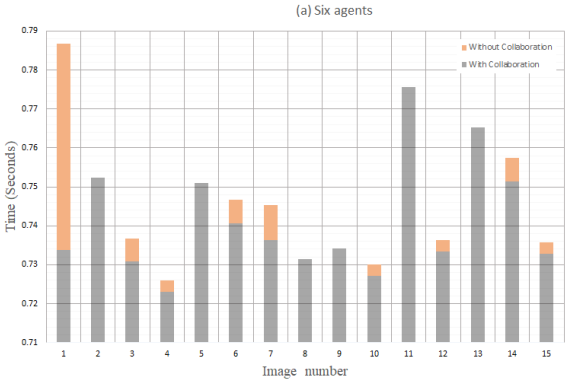

Figure 5: Time complexity for Six agents

line with uploader agent criteria (see equation 1, equation 2) after receiving other users' opinions.

Furthermore, in our multi-agent framework, negotiation between agents is introduced to improve privacy protection. Since the collaborations between agents are time-consuming, we use a coordinator agent to reduce time complexity (Figure 5). According to our negotiation model results, the coordinator agent collects whole opinions and then shares them with the target agents. Figure 5 validated the notion of using a coordinator agent with six and eight co-owners, respectively. Handling negotiations by coordinator agent reduces our prediction approach time complexity by 0.8 percent for six agents and 2.2 percent for eight agents in the agent-based collaborative privacy management.

5 CONCLUSION

In this paper, we introduced a privacy-preference negotiation approach for protecting users' privacy on online social networks. Due to the fact that users' response time takes considerable time in the standard models, we proposed an agent-based framework to maintain the popularity of online social networks. Our agent negotiation model is also applicable when users are offline. We exploited users' recent behaviors to predict their online social behaviors. Moreover, our technique utilized the co-owners opinions simultaneously. According to our evaluation, the collaboration between the associated agents caused them to provide better decisions about the shared online content. As future work, we plan to consider methods of improving the user behavior prediction for having higher opinion accuracy.

REFERENCES

[1] Gulsum Akkuzu, Benjamin Aziz, and Mo Adda. 2020. Towards consensus-based group decision making for co-owned data sharing in online social networks. *IEEE Access* 8 (2020), 91311–91325.
[2] Shaukat Ali, Azhar Rauf, Naveed Islam, and Haleem Farman. 2019. A framework for secure and privacy protected collaborative contents sharing using public OSN. *Cluster Computing* 22, 3 (2019), 7275–7286.
[3] Jundong Chen, Ankunda R Kiremire, Matthias R Brust, and Vir V Phoha. 2014. Modeling online social network users' profile attribute disclosure behavior from a game theoretic perspective. *Computer Communications* 49 (2014), 18–32.
[4] Jun Du, Chunxiao Jiang, Kwang-Cheng Chen, Yong Ren, and H Vincent Poor. 2017. Community-structured evolutionary game for privacy protection in social networks. *IEEE Transactions on Information Forensics and Security* 13, 3 (2017), 574–589.

[5] Andrew C Gallagher and Tsuhan Chen. 2009. Understanding images of groups of people. In *2009 IEEE Conference on Computer Vision and Pattern Recognition*. IEEE, 256–263.
[6] Indrasom Gangopadhyay, Anulekha Chatterjee, and Indrajit Das. 2019. Face detection and expression recognition using Haar cascade classifier and Fisherface algorithm. In *Recent Trends in Signal and Image Processing*. Springer, 1–11.
[7] Pascal Getreuer. 2013. A survey of Gaussian convolution algorithms. *Image Processing On Line* 2013 (2013), 286–310.
[8] Hongxin Hu and Gail-Joon Ahn. 2011. Multiparty authorization framework for data sharing in online social networks. In *IFIP Annual Conference on Data and Applications Security and Privacy*. Springer, 29–43.
[9] Nithya Sara Joseph. 2014. Collaborative data sharing in online social network resolving privacy risk and sharing loss. *IOSR-JCE) eISSN* (2014), 2278–0661.
[10] Anna Cinzia Squicciarini, Mohamed Shehab, and Federica Paci. 2009. Collective privacy management in social networks. In *Proceedings of the 18th international conference on World wide web*. 521–530.
[11] D. Suvitha. 2014. Mechanisms of multiparty access control in online Social network. *International Journal of Recent Development in Engineering and Technology* 2 (2014), 8–3.
[12] Deepak Tosh, Shamik Sengupta, Charles Kamhoua, Kevin Kwiat, and Andrew Martin. 2015. An evolutionary game-theoretic framework for cyber-threat information sharing. In *2015 IEEE International Conference on Communications (ICC)*. IEEE, 7341–7346.
[13] Onuralp Ulusoy. 2018. Collaborative privacy management in online social networks. In *Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems*. 1788–1790.
[14] Guido Van Rossum and Fred L. Drake. 2009. *Python 3 Reference Manual*. CreateSpace, Scotts Valley, CA.
[15] Ryan Wishart, Domenico Corapi, Srdjan Marinovic, and Morris Sloman. 2010. Collaborative privacy policy authoring in a social networking context. In *2010 IEEE International Symposium on Policies for Distributed Systems and Networks*. IEEE, 1–8.