Poster: Challenges for Assisted Audience Selection in OSN

Gaurav Misra, Jose M. Such

Security Lancaster, Lancaster University,
Infolab21, Lancaster LA1 4WA, United Kingdom.
E-mail: {g.misra,j.such}@lancaster.ac.uk

I. Introduction

Most social media users connect with people from different "life facets" such as family, work, etc., which makes audience selection an important and challenging task for day to day communication on Online Social Networks (OSNs) [1]. Users need to be able to utilize the privacy controls afforded to them by the OSNs in order to regulate access to their content and to disseminate information in a desired manner in order to avoid "context collapse".

Recent research has found that a very small minority of users create custom audiences for their content by employing the access control mechanisms available to them [2]. The findings also suggest that the users are unable to employ these mechanisms for audience selection and unintended disclosure remains largely unmitigated and can often lead to unpleasant outcomes for the users. In the perceived absence of usable audience selection mechanisms, users often employ "coping mechanisms" such as self-censorship and "un-friending" contacts on the OSNs [1]. Such drastic measures are often counter-productive and substantially diminish the utility of the OSN for the user. Thus, it is evident that users would benefit from more nuanced audience selection mechanisms in OSNs.

II. Challenges

A. Organizing Friends

One of the major problems for any audience selection mechanism is the vast amount and varied nature of contacts most OSN users have in their networks. Thus, many privacy enhancing techniques rely on efficient grouping of contacts by using community detection algorithms in order to mitigate this problem [3]. However, such communities do not necessarily reflect the users' conception of social groups. This has led to a number of recent efforts at mining "social circles" of a user's contacts based on profile features of the nodes of their social networks [4].

Popular OSNs like Google+ and Facebook have attempted to assist the users in contact management by introducing features like Circles [5] and Lists to assist them in partitioning their social network. However, as noted earlier, users fail to employ these features during audience selection and end up sharing their content with unintended audiences. This points to the fact that such techniques do not produce groups which can seamlessly translate to an audience which the user would want to select for their content. There is an evident requirement for systematic evaluations of community detection mechanisms with respect to audience selection in order to identify the most suitable approaches to assist users.

B. Dynamic Suggestions

An important requirement for any audience selection mechanism is to reduce the cognitive burden on the user by providing suggestions and assisting them in setting their privacy policies. Users of OSNs use these mediums for dynamic interactions and cannot be expected to micro-manage privacy settings for every content they post on the network.

A possible solution to this problem is to identify similar users (based on their profiles) and define access control mechanisms to multiple users at once. The current approaches of identifying similar users (such as [6]) fall short due to the method they employ to identify the suitable features for calculating similarity. It is important to select a sufficiently large set of features for the feature vector to be representative of the entire profile. However, selecting an excessive number of features can adversely affect the real-time dynamism of any mechanism which is critical in a social media environment in order to provide the user with a seamless experience. Given this obvious trade-off, a scientific evaluation to identify the optimal set of features is necessary in order to enhance the performance of audience selection mechanisms.

C. Dissemination Control

Users perform "boundary regulation in social media in order to maintain control over their data and manage their interpseronal boundaries and relationships" [1]. However, these mechanisms can be easily defeated if a recipient (even if he is intended to be part of the audience) disseminates that data after receiving it. The dissemination can result in the data reaching an unintended audience. Major OSN providers like Facebook[1] and Twitter[2] have taken steps to introduce safeguards against active dissemination of content which could potentially breach the privacy preferences of the initial content owner. Even with such safeguards, however, there are possibilities where dissemination (for example, by downloading and re-sharing the content) can lead to the content reaching an unintended audience.

[1] https://www.facebook.com/help/569567333138410

[2] https://support.twitter.com/articles/77606-faqs-about-retweets-rt#protectedtweets_notretweeted

D. Inference Control

It is possible that a user's activity on an OSN may "leak" information to recipients without their knowledge and/or consent. Even if the user is able to employ access controls to deny direct access to his content, any person in his network can potentially obtain sufficient information to infer certain details to which they have been denied access. An illustrative example is when an unauthorized user (one who has been denied access by the user) infers some hidden profile attributes from attributes that are public in the user's profile, such as his group membership and relationship links, or the profile of his/her friends [7]. To the best of our knowledge, no audience selection mechanisms have been able ot safeguard against this threat.

E. Multi-Party Audience Selection

An important challenge for any privacy management mechanism in OSNs is to consider content which is shared between multiple users (such as pictures where many user are tagged). Currently, OSNs leave the responsibility of setting a proper privacy configuration for the shared item on the owner. However, inappropriate disclosure of such data can open a breach for unauthorized, unintended dissemination, and co-privacy attacks. For any audience selection mechanism to be effective, it has to incorporate mechanisms to deal with such multi-party privacy conflicts. Many direct and indirect approaches have been discussed to solve this issue but a consensus on the best mechanism is yet to be found [8].

F. Personalized Experience

Designing access control mechanisms for OSNs is a non-trivial task if we consider the vast spectrum of privacy preferences that different individuals can have. Different users assign different amounts of sensitivity to different types of information according to their preferences and contexts. They also respond differently to interventions [9]. This suggests that a "one-size-fits-all" strategy for designing audience selection mechanisms is not sufficient.

It has also been acknowledged that user relationships are dynamic and they undergo transformations while interacting on OSNs (much like in real life) [10]. Thus, for any audience selection mechanism to have a sufficiently long-term relevance and utility for the user, it should be able to adapt to the changing dynamics of the relationships between the users and their contacts. Moreover, such mechanisms should have adaptable features in order to be universally appealing to users with different privacy preferences.

G. Improved Audience Visualization

Users often struggle to interpret complex privacy controls due to the lack of clarity of the audience visualization techniques employed. It has been found that social media users often visualize their audience in the form of social groups rather than as a collection of individuals [5]. Thus, a visualization mechanism that leverages community membership information will display the audience in a manner which is congruent with the users' conception of their social network.

An effective audience visualization technique can also enhance the possibility of overcoming some of the aforementioned challenges towards creating an effective and user-friendly audience selection mechanism. For instance, inclusion of interventions warning the users about unintended dissemination can enable them to take appropriate actions to avoid such occurrences. Moreover, the visualization mechanism can be designed in a way which readily accommodates a negotiation process with respect to shared content which can help the users overcome multi-party privacy problems. Thus, audience visualization can be viewed as the final piece of the jigsaw which any usable audience selection mechanism should prioritize in order to provide a comprehensive solution to the user.

III. Future Work

We propose the following steps in order to mitigate some of the challenges mentioned and ensure better design of audience selection mechanisms:

- Perform a systematic evaluation of community detection algorithms to identify the most suited approach for audience selection.
- Identify the subset of profile features which can sufficiently inform about user similarity in OSNs. This can be used to optimize audience selection.

References

[1] P. Wisniewski, H. Lipford, and D. Wilson, "Fighting for my space: Coping mechanisms for sns boundary regulation," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2012, pp. 609–618.

[2] P. Wisniewski, B. P. Knijnenburg, and H. Richter Lipford, "Profiling facebook users privacy behaviors," in *SOUPS2014 Workshop on Privacy Personas and Segmentation*, 2014.

[3] S. Papadopoulos, Y. Kompatsiaris, A. Vakali, and P. Spyridonos, "Community detection in social media," *Data Mining and Knowledge Discovery*, vol. 24, no. 3, pp. 515–554, 2012.

[4] A. Squicciarini, S. Karumanchi, D. Lin, and N. DeSisto, "Identifying hidden social circles for advanced privacy configuration," *Computers & Security*, 2013.

[5] S. Kairam, M. Brzozowski, D. Huffaker, and E. Chi, "Talking in circles: selective sharing in google+," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2012, pp. 1065–1074.

[6] S. Amershi, J. Fogarty, and D. Weld, "Regroup: Interactive machine learning for on-demand group creation in social networks," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2012, pp. 21–30.

[7] E. Zheleva and L. Getoor, "To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles," in *WWW '09: Proceedings of the 18th international conference on World wide web*. New York, NY, USA: ACM, 2009, pp. 531–540.

[8] A. Squicciarini, M. Shehab, and F. Paci, "Collective privacy management in social networks," in *Proceedings of the 18th international conference on World Wide Web*. ACM, 2009, pp. 521–530.

[9] Y. Wang, P. G. Leon, A. Acquisti, L. F. Cranor, A. Forget, and N. Sadeh, "A field trial of privacy nudges for facebook," in *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*. ACM, 2014, pp. 2367–2376.

[10] A. D. Kramer, J. E. Guillory, and J. T. Hancock, "Experimental evidence of massive-scale emotional contagion through social networks," *Proceedings of the National Academy of Sciences*, p. 201320040, 2014.