Predicting Privacy Settings with a User-centered Approach

Jason Watson
Department of Computer Science & Information Systems
University of North Alabama
Florence, AL USA
jwatson5@una.edu

INVITED TALK EXTENDED ABSTRACT

People are connecting and sharing large amounts of personal information through social media sites, cloud and health services, and other online applications. Users often manage their interactions and information disclosures on these sites using a variety of privacy settings. The use of privacy settings on social networking sites (SNS) such as Facebook has been extensively studied. Researchers have found that users have many friends and desire to selectively share with multiple audiences. However, users struggle to manage their privacy settings as they are quite complex and the structure of the settings changes frequently. As a result, users can share information more broadly than intended, even within the "friend" group, resulting in embarrassment or regret. Rather than adjust confusing privacy settings, users may resort to various coping mechanisms such as censoring their disclosures.

Any set of controls has a starting point---the default configuration that the user then modifies as desired. Customizing these settings takes user effort, and users often accept the defaults rather than perform the work of modifying them to meet their needs [1, 12]. Thus, the default settings can have a large impact on the resulting privacy for users [6]. For most online systems, default privacy settings are created by the developers, and are likely to emphasize the site's values for information sharing. Permissive default settings may promote social interaction but may require more user burden to manage for those with greater privacy desires. While users are able to customize these settings, many do not, at least until a privacy violation occurs. Surveys of end users have shown an increase in the awareness and modification of Facebook privacy settings over the years, yet many users still do not seem to be familiar with the extent of the privacy settings on Facebook or take the time to configure all possible settings [6]. Predicting default privacy settings that more closely represent a user's privacy preference can reduce burden by reducing the customization burden.

A. Predicting Privacy Settings

A variety of research has examined how to automatically determine or recommend personalized privacy settings. One strand of research has investigated whether measured privacy attitudes correlate to privacy settings, and thus predict settings or privacy-related behaviors. A number of privacy indexes---ranked answers from a set of privacy questions combined together as a score or classification---have been proposed. These scores can then be used to group, or segment, people into categories. The most commonly cited index is the Westin privacy segmentation model [7]. Westin segments privacy attitudes into three categories: Fundamentalists, Pragmatists and Unconcerned. Other indexes include Buchanan et al [3], Dinev and Hart [4] and Stutzman [16] which each measure privacy along multiple dimensions. However, few studies have shown that such attitudes predict or correlate to behavior.

Another approach is to learn canonical policies from existing users, to determine the default settings for new users. For example, in the location privacy domain, work with the Loccacino and PEOPLEFINDER systems seek to reduce configuration burden for dynamic and complex location privacy settings through user feedback and utilizing machine learning to generate default policies [17]. The challenge explored by such work is to determine which policy or persona a new user should have to define default sharing settings.

Others have examined using machine learning or other algorithms to automatically determine settings based on a user's previous settings or behaviors. For example, Sinha et al. gather information about users' previous Facebook posts to predict better default policies for future posts [15]. Similarly, Shehab et al. and Mo et al. suggest using machine learning to automatically configure complex privacy settings for friends based upon configuration for an initial set of friends [11, 13, 14].

Prior work on characterizing privacy includes work by Liu and Terzi who presented a framework for computing privacy scores using profile item sensitivity and the user's social network level [8]. They test two models (Item Response Theory [2] and naive) for computing privacy scores from user privacy settings. Fang and LaFevre use a privacy wizard to gather user disclosure preference to provide better default privacy settings [5]. Maximilien et al. proposed using a Privacy-as-a-Service framework to combine profile

978-1-4673-7648-8/15/$31.00 ©2015 IEEE

characteristics of sensitivity and visibility to form a privacy index that can be used to evaluate privacy risks that can be accessed using an API [9]. Similarly, Minkus and Memon examined characterizing privacy settings into a single score which can be used to aid users in configuration of the privacy policy or compare two given policies [10]. They proposed both a naive and weighted method which took into account both sensitivity and visibility. However, the underlying assumption for most of these models---based on the calculation of the characterization scores---was that profile items disclosed to a more public audience would increase privacy risk and items disclosed to more private audiences added little to no additional privacy risk. People who post information on SNS desire to share and restricting too much is at odds with the purpose of the social network site and the desire of its users.

B. A User-centered Approach

Most automated policy configuration mechanisms lack capabilities to gather additional reaction information to better characterize privacy preferences. In my talk, I discuss gathering data from participants to better characterize how privacy of shared information is viewed from the user's perspective. A limited number of participants can provide training data for automated algorithmic analysis by utilizing both the gathered sensitivity of the item and the degree to which that item fits a stated user desire without making assumptions about how that data should impact the analysis. Additionally, alternate audience privacy preferences can be used to determine privacy sensitivity in a variety of contexts. This allows for generated policies flexible enough to adjust to changing privacy attitudes as users becomes more private or more public over time.

User-centered models can be improved by properly segmenting users, for example using Westin's segmentation index. However, these indexes have not shown to be reliable in predicting user behavior and attempts to utilize these segmentation indexes have not yet been shown to be successful. In my talk, I explore the use of user-centered default policy generation and further possible improvements by using user segmentation models such as Westin's. Future work can continue to improve predicting settings by performing additional analysis on similar datasets that characterize user privacy preferences to see if there are other factors that can help determine how to segment users. In particular, data from user reported preferences can be combined with actual social activity to possibly balance the privacy paradox problem---people report to be concerned about privacy, but often disclose personal information to many people through online social activity.

Online social network interaction is dynamic and default settings are applicable to each new social interaction. Thus, more work is needed to examine how users would actually respond to such defaults, and how much effort it would take to re-configure settings for poorly predicted default settings. Finally, complex privacy settings continue to require excessive configuration burden. Future research should explore novel methods for minimizing effort. Many researchers use machine learning to predict settings from existing privacy policies that may not yet be configured by the user. I discuss the opportunity for using machine learning to complement traditional human factors research methods by learning from user characterizations and/or sharing interactions.

REFERENCES

[1] A. Acquisti and R. Gross, "Imagined communities awareness, information sharing, and privacy on the Facebook," in *Privacy Enhancing Technology*, Cambridge, United Kingdom, 2006.

[2] F. B. Baker and S.-H. Kim, Item Response Theory: Parameter Estimation Techniques, Second Edition. CRC Press, 2004.

[3] T. Buchanan, C. Paine, A. N. Joinson, and U.-D. Reips, "Development of measures of online privacy concern and protection for use on the Internet," *Journal of the American Society for Information Science and Technology*, vol. 58, no. 2, pp. 157–165, 2007.

[4] T. Dinev and P. Hart, "Internet privacy concerns and their antecedents---measurement validity and a regression model," *Behaviour & Information Technology*, vol. 23, no. 6, pp. 413–422, 2004.

[5] L. Fang and K. LeFevre, "Privacy wizards for social networking sites," in *Proceedings of the 19th international conference on World wide web*, New York, NY, USA, 2010, pp. 351–360.

[6] M. Johnson, S. Egelman, and S. M. Bellovin, "Facebook and privacy: It's complicated," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, 2012, p. 1.

[7] P. Kumaraguru and L. F. Cranor, "Privacy indexes: A survey of westins studies." Institute for Software Research International, 2005.

[8] K. Liu and E. Terzi, "A framework for computing the privacy scores of users in online social networks," *ACM Transactions on Knowledge Discovery from Data*, vol. 5, no. 1, pp. 1–30, Dec. 2010.

[9] E. M. Maximilien, T. Grandison, T. Sun, D. Richardson, S. Guo, and K. Liu, "Privacy-as-a-service: Models, algorithms, and results on the Facebook platform," in *Proceedings of Web 2.0 Security and Privacy (W2SP)*, Oakland, CA, USA, 2009, vol. 2.

[10] T. Minkus and N. Memon, "Leveraging personalization to facilitate privacy," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 2448026, Jun. 2014.

[11] M. Mo, D. Wang, B. Li, D. Hong, and I. King, "Exploit of online social networks with semi-supervised learning," in *Proceedings of the International Joint Conference on Neural Networks*, 2010, pp. 1–8.

[12] M. Mondal, Y. Liu, B. Viswanath, K. P. Gummadi, and A. Mislove, "Understanding and specifying social access control lists," in *Symposium on Usable Privacy and Security (SOUPS)*, 2014.

[13] M. Shehab, G. Cheek, H. Touati, A. C. Squicciarini, and Pau-Chen Cheng, "User centric policy management in online social networks," in *Proceedings of the IEEE International Symposium on Policies for Distributed Systems and Networks*, 2010, pp. 9–13.

[14] M. Shehab and H. Touati, "Semi-supervised policy recommendation for online social networks," in *Proceedings of the 2012 International Conference on Advances*, 2012, pp. 360–367.

[15] A. Sinha, Y. Li, and L. Bauer, "What you want is not what you get: Predicting sharing policies for text-based content on Facebook," in *Proceedings of the 2013 ACM Workshop on Artificial Intelligence and Security*, 2013, pp. 13–24.

[16] F. Stutzman, "An evaluation of identity-sharing behavior in social network communities," *Journal of the International Digital Media and Arts Association*, vol. 3, no. 1, pp. 10–18, 2006.

[17] E. Toch, N. M. Sadeh, and J. Hong, "Generating default privacy policies for online social networks," in *Proceedings of the 28th of the International Conference Extended Abstracts on Human Factors in Computing Systems*, New York, NY, USA, 2010, pp. 4243–4248.