HOW SOCIALLY AWARE ARE SOCIAL MEDIA PRIVACY CONTROLS?

Gaurav Misra, Jose M. Such

School of Computing and Communications

Lancaster University, UK

g.misra@lancaster.ac.uk, j.such@lancaster.ac.uk

Abstract: *Social media sites are key mediators of online communication. Yet the privacy controls for these sites are not fully socially aware, even when privacy management is known to be fundamental to successful social relationships.*

The use of social media sites such as Facebook, Twitter, Google+, LinkedIn, and Pinterest has grown massively over the last decade. Social media users experience many benefits, such as establishing, developing, and maintaining social relationships through shared personal information. Indeed, this plays a crucial role in managing what is known as social capital. Social media sites also enable users to build and participate in communities and networks of people who share similar interests. Even governments and politicians around the world use social media to engage with citizens. For example, the UK government encourages civil servants to use social media and provides guidelines for doing so [1], and social media arguably played an important role in the re-election of US President Barack Obama in 2012 [2].

Despite social media's unquestionable success, privacy concerns have been increasing over the past few years. Sharing personal information with unintended audiences (commonly referred to as the "insider threat") is of particular concern. This is especially problematic with sites that treat all of a user's "friends" in the same manner—for example, without differentiating between close friends and professional colleagues. Along with other variables such as location, topic, and time, the social context of a particular disclosure forms a very significant part of that disclosure's overall context. For example, if a user is posting about an event in his personal life, he might choose to deny access to his colleagues. The context here is defined by the topic of the disclosure as well as the type of social relationship the user has with the audience. This helps the user determine the appropriate audience for that disclosure, ensuring maintenance of contextual integrity [3] and enabling regulation of dynamic social boundaries [4]. Thus, acknowledging and accommodating such social contexts is imperative to safeguard the privacy of social media users. This raises the question: How socially aware are current mainstream social media privacy controls?

Classification of Mainstream Social Media Privacy Controls

We used Alexa's traffic rankings to identify the top 30 social media sites [5] and clustered them into categories offering similar support to model social contexts. We excluded dating sites, online shopping sites, and sites that were too specific to particular populations (for example, Classmates for US graduates and Naijapals for Nigerians). Figure 1 shows the classification of the top 30 general-purpose social networking sites. We evaluated the individual social media

This is the accepted version of the paper. The reader is referred to http://ieeexplore.ieee.org/abstract/document/7433361/ for the published version in IEEE Computer, volume:49, Issue3, 2016.

infrastructures by looking at each site’s privacy policies and settings. In most cases, we created user accounts to examine the actual available options for users, because this information wasn’t directly evident from privacy policies. We created sample user accounts using different email addresses and experimented with each infrastructure’s various access control mechanisms. In our evaluation, we encountered the following types of mechanisms.

Binary Classification

Nearly half (14) of the sites we evaluated were found to have a binary distinction between a user’s friends and the rest of the network. This means that the only relationship type is “friends,” with no granularity. In these scenarios, a user is unable to distinguish between two friends, which doesn’t reflect real-life social relationships.

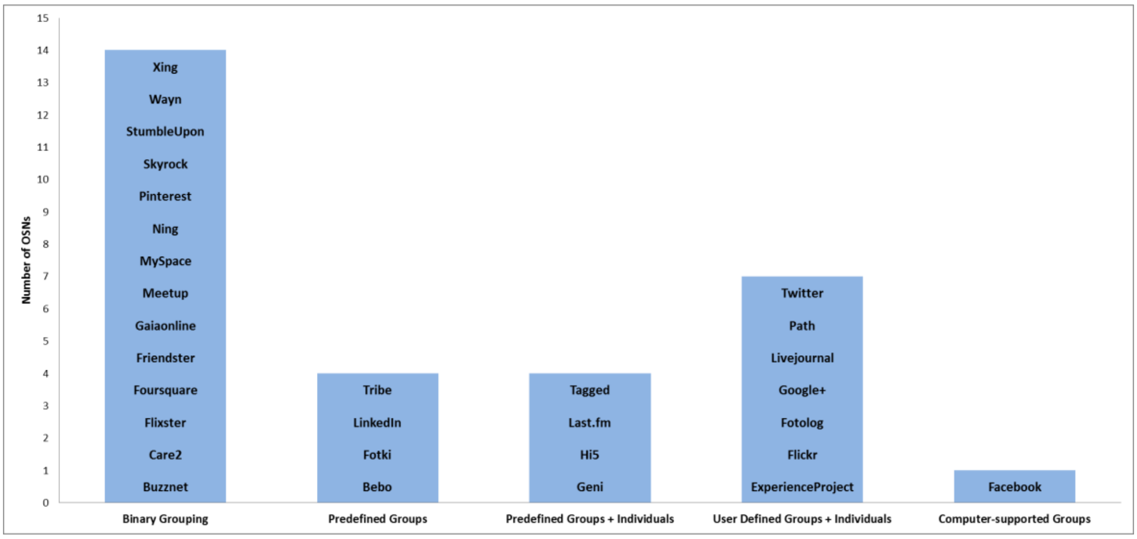

Figure 1. Top OSNs classified according to the social aspect of their privacy controls and ordered alphabetically for each level as of January 2015.

Predefined Groups

Some sites, such as LinkedIn, allow for predefined groups, which help users organize their contacts. Users can create groups (for example, “colleagues” or “family”) and then treat these groups differently. However, there’s no option to make exceptions. For example, a user can’t share a post with everyone in the “family” group except one or two individuals—the post will be seen by all members of that group. We found four sites with this type of privacy mechanism.

Predefined Groups + Individuals

An improvement is found in sites such as Tagged and hi5, which provide the option of treating individuals separately from predefined groups. This helps users share content in a more realistic way. For example, a user might have a group for “colleagues” but might not want each member to see every post. This type of mechanism allows for more granularity and user control.

User Defined Groups + Individuals

Another enhancement is allowing users to create their own groups. Google+ and Facebook both provide default groups but also allow users to manage their own circles and lists per individual, more closely reflecting real- life relationships.

Computer Supported Grouping

We list Facebook separately in this classification because its privacy controls provide an enhanced grouping mechanism that other social media sites don't offer. Facebook's "smart lists" feature allows users to create lists based on features like location and workplace. Also, the introduction of the "close friends" and "acquaintances" lists acknowledges the important role of relationship strength.

Relationship-Based Access Controls

Mainstream social media seems to be moving toward more socially aware privacy controls, which shows recognition of the importance of privacy in social relationships. However, there's still room for improvement to make privacy controls more socially aware.

Traditional access control approaches such as role-based access controls or group-based approaches can't truly capture the social relationships among users—relationship-based access controls (ReBACs) are needed [6]. A ReBAC model uses a different set of properties to define relationships, resulting in a more natural disclosure of personal information. For example, users can decide that only their close friends can see a specific photo.

One of the main problems facing ReBACs is usability. The ReBAC model considers a large number of social features, which can help users better identify the social context of their disclosures; however, the process of defining relationships and selecting audiences needs to be easy. This entails improving audience visualization—the visual cues provided to a user about which friends will have access to the information the user posted or is about to post. Moreover, ReBACs need to be computationally lightweight and to seamlessly integrate with the social media interface, preserving the dynamism of users' social networking experiences. A recent effort to implement a ReBAC mechanism uses attribute-based encryption that allows users to control access to their photos on an iOS platform [7].

In our analysis of privacy controls, we noticed a glaring absence of mechanisms allowing multiple users to negotiate access control decisions for items that involve them, such as pictures and posts, before these items are posted [8]. Most privacy controls apply the privacy preferences of the user making the post. However, if an affected user wants the post removed, he or she must negotiate with the poster using other means of communication such as email, texts, or private messages. Even then, negotiations might happen after the item has been already posted and a privacy violation has occurred.

Computational mechanisms that automate the negotiation process have been identified as a possible mitigation. This doesn't mean that users would lose control; instead, these mechanisms would suggest possible solutions that all parties would need to accept. If users don't accept the suggestion, they need to enter into a manual negotiation by other means. The main challenge is to propose solutions that everyone involved will accept most of the time.

Some mechanisms have been proposed in this very young discipline, but a more formal study is required to understand the conditions under which users will make concessions, and the variables that make users take stronger or more lenient positions during these negotiations.

Another open challenge is the ability of privacy controls to adequately support users in making favourable disclosure decisions with regard to self-presentation and management of relationship dynamics. Users maintain different types of relationships with varying objectives, and the manner and content of their communication with these groups varies accordingly. These nuances must be adequately accommodated and supported, which poses many sociotechnical challenges for future research on the topic. One particular challenge is the development of tools that are aware of relationship status, including the user's disclosures as well as reciprocations provided by other network members [9]. This information would provide the intelligence for a decision support system, which would help users understand their relationships and fine-tune their information disclosures. A learning mechanism would be required so that these systems could understand each user's behavior and adapt accordingly to provide relevant assistance. One major concern is that such systems could become too intrusive, as they observe and analyze all communications between users.

Except for a handful of distributed social media sites that are implemented by peer-to-peer nodes, the provider mediates communication on most of these sites. Thus, the provider can influence the amount and nature of communication between individuals on its platforms. For example, a recent experiment studied the emotional contagion of Facebook status updates by moderating the amount of content received by users from various friends [10]. This confirms that the provider can modify the content being fed to the user through the network, which can alter the nature and strength of relationships that depend on interactions between individuals. This also highlights the fact that institutional privacy—which governs the way social media providers handle user data, including whether and how they will share data with third parties—can play a role in social privacy [11].

Conclusion

Mainstream social media seems to be moving toward more socially aware privacy controls. However, these efforts are still a long way from the comprehensive modelling of social relationships that would enable satisfactory boundary regulation, mimicking peoples' relationships in the offline world. Current research advances in this area will lead to the development of next-generation privacy controls. These new privacy controls will, like any new technology, be a double-edged sword. They will empower users to manage their privacy online in unprecedented ways, but they could also enable potentially hazardous, privacy-invasive practices, such as more accurate targeted advertising or the monetization of social relationship information. We must find an adequate balance between institutional and social privacy to protect users at both levels.

References

[1] UK Government, "Social Media Guidance for Civil Servants: October, 2014," 20 October 2014. [Online]. Available: www.gov.uk/government/publications/social-media-guidance-for-civil-servants. [Accessed 1 December 2014].

[2] Pew Research Center, “How the Presidential Candidates Use the Web and Social Media,” 15 August 2012. [Online]. Available: www.journalism.org/2012/08/15/how-presidential-candidates-use-web-and-social-media. [Accessed 25 November 2014]

[3] Nissenbaum, Helen. "Privacy as contextual integrity." Washington law review 79.1 (2004).

[4] Palen, L., & Dourish, P. (2003, April). Unpacking privacy for a networked world. In Proceedings of the SIGCHI conference on Human factors in computing systems (pp. 129-136). ACM.

[5] Alexa.com, “Top Sites in Social Networking,” [Online]. Available: www.alexa.com/topsites/category/Computers/Internet/On_the_Web/Online_Communities/Social_Networking. [Accessed 15 October 2014]

[6] Fogues, Ricard, et al. "Open Challenges in Relationship-Based Privacy Mechanisms for Social Network Services." International Journal of Human-Computer Interaction just-accepted (2015).

[7] Yuan, Lin, et al. "Privacy-preserving photo sharing based on a public key infrastructure." *SPIE Optical Engineering+ Applications*. International Society for Optics and Photonics, 2015.

[8] 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.

[9] Such, Jose M., Agustín Espinosa, Ana García-Fornes, and Carles Sierra. "Self-disclosure decision making based on intimacy and privacy." *Information Sciences* 211 (2012): 93-111.

[10] Kramer, A. D., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. Proceedings of the National Academy of Sciences, 111(24), 8788-8790.

[11] Gurses, Seda, and Claudia Diaz. "Two tales of privacy in online social networks." *Security & Privacy, IEEE* 11.3 (2013): 29-37.