Andrew McNeill, Lynne Coventry (2016):
"Even in a group I'll not tell them all": Understanding privacy concerns of older adults for designing online social networks.
In Markus Garschall, Theo Hamm, Dominik Hornung, Claudia Müller, Katja Neureiter, Marén Schorch, Lex van Velsen (Eds.),
International Reports on Socio-Informatics (IRSI),
Proceedings of the COOP 2016 - Symposium on challenges and experiences in designing for an ageing society.
(Vol. 13, Iss. 3, pp. 78-84)

# "Even in a group I'll not tell them all": Understanding privacy concerns of older adults for designing online social networks.

Andrew McNeill and Lynne Coventry

PaCT Lab, Northumbria University, Newcastle Upon Tyne

andrew.mcneill@northumbria.ac.uk,
lynne.coventry@northumbria.ac.uk

**Abstract.** In this paper we explore the challenge of obtaining privacy requirements for online social network systems (SNSs) designed for older adults. Since privacy concerns are purported to be a barrier to SNS uptake among older adults, it is important to design to address these. Unique challenges include the fact that older adults may not be familiar with online SNSs and may not understand existing options to optimise privacy on SNSs. Previously, disclosure grids have been used to understand information disclosure but a more appropriate way to identify privacy requirements may be through participant designed sociograms. Nevertheless, even this approach comes with challenges since privacy is an internal issue regardless of their connection to specific groups of friends. We suggest the possibility of trust-based network arrangements and discuss how these might adapt to information-types and how they might present feedback to older adult users to make privacy settings transparent.

# 1 Introduction

A key obstacle for use of online SNSs by older adults is said to be privacy concerns (Nef et al., 2013; Xie et al., 2012). Older people are often exposed to media reports of young adults' online indiscretions and resultant problems. Why would older adults enter a world where privacy appears to be obsolete? If adoption is to be increased within this demographic, design of such networks must place users' privacy concerns at the forefront of the design process to ensure that consequences of using these products are acceptable to older adults.

There are unique challenges facing researchers when working with older adults to uncover privacy requirements for SNSs. For example, older adults typically use SNSs less than the rest of the population (Perrin, 2015) and when many of them are asked about privacy on SNSs, they may not have a clear understanding of why they would use them, the risks present or the privacy protections available. Those who do use SNSs are not always aware of the privacy settings available or how to control them (Gibson, Moncur, Forbes, Arnott, & Martin, 2010; Madden, 2012). It has also been found that only a small number of users change the initial privacy settings, which often default to maximum visibility, not privacy (Gross & Acquisti, 2005). For these reasons, discussing the potential for privacy features in a new SNS for older adults can be difficult.

# 2 Research Context

Our context for developing user-led privacy features in an online SNS is the ACANTO project (http://www.ict-acanto.eu/). The aim is to improve the wellbeing of older adults (classified here as people over 65 years) through the combination of an intelligent walker to improve physical mobility, an SNS to develop social contacts, and a recommendation system to generate personalized ideas for activities (combining the physical with the social (e.g. recommendations to go out with a friend). Since the system may collect substantial amounts of data (e.g. physical activity, health indicators, emotional state, activities, social contacts), privacy concerns are significant. Potentially, such a system will feed some information to medical professionals to monitor behaviours that may provide an early warning of decline in an older adult who, for example, has not left the house for several days. Older adults may not want such data to be shared and therefore their privacy preferences related to the dissemination of such data will need to be made clear. The research reported here was conducted as a pilot study with 6 older adults (5 female, 1 male; mean age = 71.3 years) who conducted interviews about privacy among their friends. Some of the users had used online SNSs previously and all were familiar with the concept. The results of

these interviews were reported to developers of the SNS whom we collaborate with to develop the SNS.

# 3 Disclosure grids

One way in which privacy preferences have been explored previously is through information disclosure grids (Little et al., 2011). This technique asks participants about willingness to disclose different types of information to different groups. In the grid, one axis lists information types (e.g. medical information, financial details, or employment details) and the other axis lists groups (e.g. doctor, partner, or work colleagues). Participants indicate what information they would disclose to each group. This research has shown, for example, that users are more willing to disclose personal identity information (e.g. name and date of birth) than other types. Furthermore, applying the technique to a sample with a large age-range reveals that younger and older members of society are less protective of a range of information compared to middle-aged participants (Little et al., 2011). While younger and older participants were nonchalant about privacy by saying that they had nothing to hide, this may also indicate a lack of awareness of privacy-risks. If so, then this highlights the need to communicate privacy risks to participants when discussing privacy concerns during design-research. Simply asking about privacy concerns may not elicit complete responses if the risks of information disclosure are not fully known.

Nevertheless, the information disclosure grid technique is simple to apply and creates clear paths for information sharing between groups. Developers can design systems to ask older adults what types of information they are happy to share with specific groups of friends and this can serve as a privacy profile. However, because the approach may use a priori categories of groups that information will be shared with, a more inductive approach may be necessary to fully elicit requirements from users.

# 4 Sociograms

To develop a more inductive approach to privacy requirements-generation for online SNSs, we have used participant generated sociograms to create diagrams of participants' offline social networks in order to ask them about information-sharing preferences. Participant-aided sociograms (Hogan et al., 2007) are produced by asking participants to write down lists of the names of all their friends, categorise those friends by closeness, arrange the friends in concentric circles around themselves at the centre, and then draw lines around friends to

show groups and lines between friends to show connections. This approach ensures that the identification of groups is inductive (i.e. they identify their own groups of friends) and subsequent questions about privacy can then be tailored to ask about information sharing with each of those groups. In our study, friends were grouped according to activities (e.g. dancing group, bowling club or quiz group) and after participants had produced these diagrams we asked questions about what types of information they would share with each group of friends. We had a list of information types that would potentially be used by the system (e.g. location, emotional state, and health information) and these were described to the user who was then asked what groups or individuals they would allow to see the information.

Because the construction of sociograms represents a social network, it is an ideal way of asking about privacy concerns within an SNS. Participants found it easy to identify people and groups that they would or would not share specific information with. Also, because the groups of friends were inductively generated, it was a more appropriate way of generating requirements for the proposed SNS. Nevertheless, the approach revealed some challenges for SNSs.

Firstly, simply because someone is a member of a group of friends does not mean that everyone in that group is privileged with the same information. Even when a group was seen as close, individuals within the group could be described as “nosy” and were excluded from knowing some things. Secondly, information is shared for specific purposes. With regards to health information, some people wanted to share it widely as a way of gaining support and understanding. For others, health information is hidden from family out of concerns that it might worry them. It is thus too simplistic to say that certain groups will always receive certain types of information. Thirdly, (lack of) trust seems to be a bigger privacy moderator than group membership. One participant, talking about information sharing, said, “It’s like a trust thing isn’t it? You know you build up trust. So everybody is different and even in a group I’ll not tell all of them what’s happening”. Clearly then, the sociogram approach highlights the issue of interpersonal trust which information disclosure grids did not. So how can we explore trust more fully?

# 5 Networks of trust

If we envisage information disclosure as a social contract in which we expect procedural fairness (including privacy and acceptable use of the information), then trust has a role to play in determining who we will enter this contract with. Just as trust in the SNS itself affects usage among older adults (Braun, 2013), so also trust can be expected be affect the sharing of information within the social network. Furthermore, it may be possible to envisage trust as a grouping category

rather than activities or group membership (Müller, Hornung, Hamm, & Wulf, 2015). We intend to conduct further research in which we ask participants to produce sociograms, not arranged by "closeness", but by levels of trust. Furthermore, we can produce these sociograms using technologies such as NetCanvas (http://networkcanvas.io/) which allows users to reconfigure their networks based on different criteria (Hogan et al., 2016). In this way, participants can be asked to reconfigure their networks based on their trust of others to be recipients of different types of information. Culnan and Armstrong (1999) identify 4 reasons why people may trust people with information which may help understanding these trust groups: (1) there is an existing relationship (2) they perceive they can control future use of the information, (3) the information is relevant to the relationship and (4) they believe the information will be used to draw reliable and valid inferences about them and will be acted on appropriately. The reasons given for the arrangement of nodes will help explain why some people are more trusted than others with specific information and whether there are simple ways of asking questions that would identify recipients of different information. These criteria of trust can be reported to developers who can design the system to ask users who register to arrange their contacts based on the criteria of trust.

The configurable nature of networks produced in tools such as NetCanvas generates clearer visualisation of privacy settings by older adult users than typically allowed in SNSs insofar as users can see who in their networks see what types of information. Thus, as a design-research tool they are ideal as it is clear to older adults the precise meaning of social network structures and privacy with respect to specific information-types.

Yet even with this arrangement of a network by trust, it still does not deal with the dynamic nature of privacy. While family members might be trusted with health information in general, they may be excluded from specific facts to protect them from worrying. They are trusted, but other considerations affect privacy concerns. In order to probe these issues, participants need to be asked more specific questions, perhaps even given specific examples of information that would be shared with people in their trust networks. Using concrete examples will help to uncover the additional concerns that affect privacy aside from trust. And in the same way as scenarios have proved to be useful in privacy research (Ackerman, Cranor, & Reagle, 1999), concrete scenarios where users are asked to imagine specific information being shared with specific people will enable more precise reflection on when other moderators, aside from trust, are utilised.

# 6 User-feedback

One important feature of designing an SNS for older adults is feedback on the privacy settings. This has been a problem for many users, and particularly for older adults (Gibson et al., 2010). But even on ethical grounds, informed consent requires that users be fully aware of what information will be shared, with whom and for what purposes. Perhaps the solution is to present privacy settings in the same way as we suggest generating them - through the presentation of a trust sociogram. That way users can see exactly who sees what types of information. Furthermore, being able to easily configure the trust-levels of "friends" would enable users to dynamically change privacy configurations based on changing relationships with those on their SNS. The utility of sociograms in enabling potential users to think about their online SNS structure and relationships would provide insight into whether this is a good way of presenting this data to users.

# 7 Conclusion

In conclusion, we argue that designing SNSs for older adults requires attention to the levels of trust that older adults have towards others. Such levels of trust can be conceptualised in sociograms that show participants who they share information with so as to enable them to think precisely about whether they have privacy concerns with such sharing. Sociograms are a design-solution for researchers that enable older adults to think clearly about privacy. Futhermore, if sociograms are used as feedback to show SNS users their privacy settings, then this requires developers and designers to conceptualise the privacy settings of users in the same way as users conceptualise them. This shared "mental model" of the network between users, designers and developers ensures a coherent understanding of the system. In this way a user-centered approach to privacy is communicated throughout the entire project team.

# 8 Acknowledgements

This project was funded by European Union Horizon 2020 Research and Innovation-Societal Challenge 1 (DG CONNECT/H): grant agreement No 643644

# 9 References

Ackerman, M. S., Cranor, L. F., & Reagle, J. (1999). Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences. In Proc. of the 1st ACM conference on Electronic commerce - EC ’99 (pp. 1–8).

Braun, M. T. (2013). Obstacles to social networking website use among older adults. Computers in Human Behavior, 29(3), 673–680.

Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. Organization Science, 10, 104–115.

Gibson, L., Moncur, W., Forbes, P., Arnott, J., & Martin, C. (2010). Designing Social Networking Sites for Older Adults. In Proc. of the 24th BCS Interaction Specialist Group Conference (pp. 186–194). British Computer Society.

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In WPES 05 (pp. 71–81).

Hogan, B., Carrasco, J. a., & Wellman, B. (2007). Visualizing Personal Networks: Working with Participant-aided Sociograms. Field Methods, 19, 116–144.

Hogan, B., Melville, J., Phillips II, G., Janulis, P., Contractor, N., Mustanski, B., & Birkett, M. (2016). Evaluating the Paper-to-Screen Translation of Participant-Aided Sociograms with High-Risk Participants. In CHI 16. ACM.

Little, L., Briggs, P., & Coventry, L. (2011). Who knows about me?: an analysis of age-related disclosure preferences. BCS-HCI ’11 Proc. of the 25th BCS Conference on HCI, 84–87.

Madden, M. (2012). Privacy management on social media sites. Pew Research Center.

Müller, C., Hornung, D., Hamm, T., & Wulf, V. (2015). Practice-based Design of a Neighborhood Portal. In Proc. of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI ’15 (pp. 2295–2304). New York, USA: ACM Press. http://doi.org/10.1145/2702123.2702449

Nef, T., Ganea, R. L., Müri, R. M., & Mosimann, U. P. (2013). Social networking sites and older users - a systematic review. International Psychogeriatrics, 25, 1041–53.

Perrin, A. (2015). Social Media Usage: 2005-2015. Pew Research Center.

Xie, B., Watkins, I., Golbeck, J., & Huang, M. (2012). Understanding and Changing Older Adults’ Perceptions and Learning of Social Media. Educational Gerontology, 38, 282–296.