Proceedings of the Mobile Privacy and Security for an Ageing Population workshop at the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI) 2018, Barcelona, Spain

Summary

This one-day workshop, funded by the Cybersecurity Across the Lifespan (cSALSA) project, was co-located with MobileHCI 2018 at Universitat Pompeu Fabra's Ciudadela Campus (Barcelona, Spain), and ran on Monday 3rd September 2018. The purpose of the workshop was to identify key privacy and security challenges on mobile devices as people age, and address how to resolve these issues in an inclusive manner. It addressed mobile technologies beyond smartphones and tablets to include wearables and IoT. Through a number of activities, participants worked towards understanding the interplay between ageing and privacy/security issues with the aim of informing future research and design in the increasingly ubiquitous mobile landscape. Perhaps most importantly, attendees engaged in discussions with like-minded researchers with the prospect of establishing long-term relationships and collaborations.

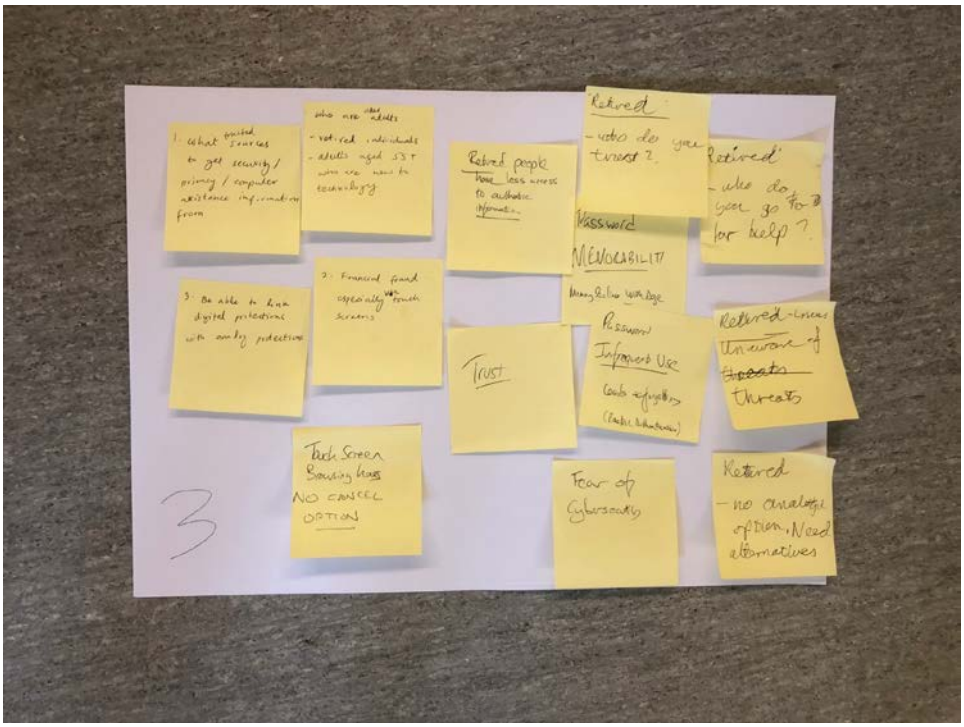
Potential attendees were invited to submit short position papers or posters related to the topic, offering either challenges or solutions. Nine papers and one poster were accepted and were made available on the workshop website. Financial support of up to €250 was offered to PhD students and Early Career Researchers to cover registration, travel, and accommodation for attending the workshop.

On the day, the workshop consisted of four sessions.

Session1
The first session of the workshop consisted of 5-minute (plus 2-minute questions and answers) paper presentations.

Session 2

The second session of the workshop consisted of group work identifying the key challenges that older adults face in the context of mobile privacy and security. Participants were randomly assigned to one of three groups and were asked to discuss and list challenges that they personally looked to address, but also other challenges that were necessary to acknowledge.



For the first half of the session participants were asked to stay within their groups, but they were allowed to roam amongst groups for the second half.

Original groups were given time to report back on their key challenges to the workshop. All key challenges were then collated by the organisers (see Challenges Identified below) and presented to attendees for a vote. Every attendee was given two votes: one for a first-choice challenge to tackle in the upcoming sessions, and one for a second-choice challenge. Organisers collected and tallied the votes.

The two challenges to be explored in more detail were: Issues with Authentication and Trust Issues and Fear of Cybersecurity.

Session 3

The third session consisted of participants exploring one of the challenges in more detail. Participants were randomly assigned into two groups (different from the morning groups) and given a challenge to discuss.

Each participant was given a role to play (a different hat, based on DeBono's Six Thinking Hats).

Session 4

The fourth session consisted of the two groups exploring the other challenge. During this session, participants were allowed to discuss concepts without any constraints (e.g. no Thinking Hats).

The two groups were given 10 minutes each to report on their ideas and approaches for addressing both key challenges.

Post Workshop

A subset of workshop attendees attended a funded dinner at La Ciudadela Restaurant where some follow-up conversations took place.

Thanks to everyone who joined us!

Attendees

Bilal Ahmad (University of Limerick, Ireland)
bilal.ahmad@ul.ie

Florian Alt (Bundeswehr University Munich, Germany)
florian.alt@ifi.lmu.de

Agon Bexheti (University of Lugano, Switzerland)
agon.bexheti@usi.ch

Barbara Corsetti (University Carlos III of Madrid, Spain)
bcorsett@ing.uc3m.es

Lothar Fritsch (Karlstad University, Sweden)
lothar.fritsch@kau.se

Yousra Javed (Illinois State University, USA)
yjaved@ilstu.edu

Jake Pywell (Northumbria University, UK)
jake.pywell@northumbria.ac.uk

Ken Scott-Brown (Abertay University, UK)
k.scott-brown@abertay.ac.uk

Ingvar Tjøstheim (Norwegian Computing Center, Norway)
ingvar.tjostheim@nr.no

Organisers Present

Emily Collins (University of Bath)
e.i.m.collins@bath.ac.uk

Chiara Lunerti (University of Kent)
c.lunerti@kent.ac.uk

James Nicholson (Northumbria University)
james.nicholson@northumbria.ac.uk

Challenges identified:
All challenges from the group activity were collated to form the following ten challenges.

1. Issues with authentication (e.g. memorability, accessibility)

2. Access control alternatives (e.g. for facilitating technical help) & accountability

3. Perceptions of susceptibility

4. Support mechanisms for older adults (both formal and informal)

5. Constant change of technology and frustration (e.g. updates, processes)

6. Explaining difficult concepts (e.g. the cloud) and difficulties explaining need for privacy and security

7. Who is an older adult?

8. Independence and dignity

9. Implications of touch screens for privacy and security

10. Trust issues and fear of cybersecurity (e.g. bad experience can lead to fear and withdrawal)

Pathways to addressing challenges

Issues with Authentication

Group 1

Graphical passwords were discussed as an alternative to traditional passwords, due to better memorability (biggest issue that older adults face)

Multifactor authentication was also discussed as a possible solution to authentication issues. By using voice recognition as the first factor (due to older adults' familiarity with voice – e.g. phone use) and a personal assistant (i.e. Alexa) as a second factor. The second factor would serve as a challenge-response natural language authentication mechanism.

Usable two-factor authentication was discussed. Using something physical that older users have (or use) regularly as a second factor seems like a good idea, although difficult to establish what that might be (e.g. button in the home?).

Group 2

Encouraging older users (and everyone!) to use password managers seen as a possibility for reducing the memorability issues. This would probably be through education, although establishing the best methods for communicating this information, and understanding any usability challenges that arise from their adoption are to be determined.

Some older adults are in a position where they rely on carers to help them with device troubleshooting or with online purchases. These processes require the users to authenticate, and in some instances for the carer to authenticate on behalf of the user. Different levels of access may be a possible solution to these issues, where the user is able to pass on credentials that limit the carer to only some functions of the device, or where a spending limit applies (and may lack privileges for certain apps, e.g. mobile banking).

Discussion over giving older users a choice over which modalities to use for authentication and what backups to have available were particularly interesting, and in the spirit of an inclusive solution to authentication issues. Future work would have to explore what modalities users are likely to choose and for what reason – and whether these reasons are actually valid.

Trust Issues and Fear of Cybersecurity

Group 1

Discussions over potentially developing a social network for older adults to discuss cybersecurity concerns, practices, and tools. The motivation behind this idea is that older users may find discussions with like-minded individuals who are in similar situations more useful than discussions with random people who may have much different living situations.

A trustworthy third party body to inspect apps/services was suggested to reduce older adults' fear of cybersecurity. Perhaps something along the lines of Which? In the UK (but with a cybersecurity focus) or perhaps a response column in a website or newspaper (again, focused on cybersecurity).

An alternative term to “cybersecurity” was suggested in order to make the concepts less daunting. Developing two-way authentication (websites authenticate to users, as well as users authenticating to websites) was also discussed.

Group 2

Discussions over potentially developing a social network for older adults to discuss cybersecurity concerns, practices, and tools. The motivation behind this idea is that older users may find discussions with like-minded individuals who are in similar situations more useful than discussions with random people who may have much different living situations. (Coincidentally same as Group 1)

A trustworthy third party body to inspect apps/services was suggested to reduce older adults’ fear of cybersecurity. Perhaps something along the lines of Which? In the UK (but with a cybersecurity focus) or perhaps a response column in a website or newspaper (again, focused on cybersecurity). (Coincidentally same as Group 1)

Discussions over people in academia becoming consumer champions for the people. They can use stories and analogies (instead of data) to get things implemented, and to engage with community groups. Academics should be trusted, but they do not have a billion-dollar voice (like corporations).

Future research interests

Issues with authentication:
Agon B. (2-factor w/voice), Bilal A., Chiara L., Lothar F., James N., Ken S-B

Access control alternatives & accountability:
Lothar F.

Support mechanisms for older adults:
James N.

Constant change of technology and frustration:
Barbara C.

Explaining difficult concepts and difficulties explaining need for privacy and security:
Bilal A., Chiara L., Emily C., Lothar F., James N.

Independence and dignity:
Emily C.

Implications of touch screens for privacy and security:
Barbara C., James N., Yousra J.

Trust issues and fear of cybersecurity:
Bilal A., Emily C., Lothar F.

Phishing training materials for seniors / financial fraud prevention:
James N., Yousra J.

Elderly acceptance of identification smart systems:
Barbara C., Chiara, L.

About Cybersecurity Across the Lifespan (cSALSA)

Partners:
University of Bath: Prof. Adam Joinson, Dr. Simon Jones
Cranfield University: Dr. Darren Lawrence
Northumbria University: Prof. Pam Briggs, Prof. Lynne Coventry
University of Portsmouth: Prof. Debi Ashenden

Project Information:
The Cybersecurity Across the Lifespan (cSALSA) project seeks to study cybersecurity behaviour amongst three main groups: young people (under 16 yrs), working age, and older adults.

The project takes a three-pronged approach to studying cyber security dynamics across three life stages: firstly, investigating the way cyber security is understood and framed in language across the lifespan and between experts and laypeople. This gives us a better understanding of the way cyber security is negotiated in context and as an everyday 'hassle' but it also gives us the opportunity to create a properly grounded dictionary of cyber security features for use in computational linguistic studies of corpora. Secondly, conducting in-depth work at the three life stages, using digital living as our focus for social and technological change and cybersecurity attitudes behaviours as an emerging response to that change. Finally, by proposing the use of insights from both the language and the observational/ethnographic work to develop new psychometrically validated measures of perceived cyber security risks, hassles and behaviours. These measures will be grounded in the everyday discourses that exist around cybersecurity and will enable the team to develop a more systematic understanding of the ways that these challenges are both perceived and met across the lifespan. The project has the following objectives:

1) To study the definition and meaning of security and cyber security in everyday language.
2) To develop and test a dictionary of cyber security related features.
3) To investigate different cyber security attitudes and behaviours across the lifespan, with specific focus on the role of context and life stage on determining threat perception and behaviour.
4) To develop a psychometrically valid measure of cyber security attitudes, behaviour and risk propensity suitable across contexts and life stage, and metrics for use in the workplace.
5) To apply this knowledge to cyber security educational and training materials in the workplace and as designed for the general public.

cSALSA is funded by the Engineering and Physical Sciences Research Council (EPSRC) and will run for 36 months from Spring 2017.

Accepted Papers

Older Adults' Interaction with Mobile Devices in Ireland: A Survey

Bilal Ahmad
Lero, the Irish Software Research Centre, University of Limerick, Ireland
bilal.ahmad@lero.ie

Simon McLoughlin
IBM Damastown Campus, Dublin, Ireland
simonmcloughlin@ie.ibm.com

Ita Richardson
Lero, the Irish Software Research Centre, University of Limerick, Ireland
ita.richardson@lero.ie

Sarah Beecham
Lero, the Irish Software Research Centre, University of Limerick, Ireland
sarah.beecham@lero.ie

Abstract
Mobile Devices can be beneficial for older adults (OAs) if used effectively. Yet current research suggests a low level of take-up. We investigated the extent to which OAs use mobile devices to identify their likes, dislikes and expectations in order to find new ways to increase their interaction. We conducted a survey with 202 OAs (aged 50-86). Many OAs are using mobile phones for communication and information seeking technology. However, without asking a direct question, privacy concerns were raised as a potential barrier towards adoption. When designing mobile apps, privacy must be a primary consideration and built in feature.

MobileHCI '18, September 3-6, 2018, Barcelona, Spain.

Author Keywords
Older adults; mobile devices; privacy; survey.

ACM Classification Keywords
H.5. m. Information interfaces and presentation (e.g., HCI): Collaborative and social computing systems and tools: social networking sites.

Introduction
Virtually every country in the world is experiencing growth in the number and proportion of OAs [15]. Similarly, in Ireland, there has been a 19.1% rise in the population of OAs since 2011 and the 50+ group are now larger than any other age group [9]. In our research, we have set 50 years as the threshold at which someone is termed an OA as defined by the World Health Organization [17]. Also, it is after this age that lifestyle changes are observed, such as family members moving away, number of friends decreasing, age discrimination within the workplace, early retirement and bereavement [16]. The increase in longevity is to be welcomed, but with it come responsibilities. As a community, we need to ensure this segment of the population remain healthy and engaged [1]. A problem with OAs is social Isolation and loneliness, which can be detrimental to their physical and mental health [4], eventually leading to a low quality of life [5].

1. Define the Research Question: Through studying existing research, we defined one high level research question: "How do older adults in Ireland interact with mobile devices?" Our rationale is the need to build on existing knowledge rather than expect people to change and learn new tools and functionality. We also wanted to highlight OAs' likes, dislikes and expectations from such devices.

2. Define Sample and Variables: We used an opportunistic approach to selecting our sample. Our unit of analysis was the older adult. Some of the common characteristics of participants include aged over 50, living in a community, having access to internet and a basic knowledge of technology. The independent variables analyzed were residence, education and living arrangements. Dependent variables included, usage, likes and dislikes.

Mobile devices such as mobile phones and wearables provide a potential solution to the problem of social isolation. They can help OAs stay connected and encourage active lifestyles [11, 12]. We noted during our review of the literature on social network systems (SNSs) for OAs [2], several barriers to technology adoption such as difficulty in operation, lack of purpose and confidentiality with privacy on the top of the list. "Privacy is a major concern and should be managed in any system developed for OAs [13,18]". The review notes that OAs are very sceptical about SNSs and are concerned that their personal information may be accessed by someone other than the intended person. A considerable amount of research has been undertaken to understand the interaction of OAs with computational technologies [7], with a focus on social media [8], websites [10] or apps [3]. Yet, what remains unclear is the actual up-take of mobile devices by OAs [6, 14,]. We, therefore, have conducted an online survey (http://bit.do/seniormobiledeviceuse) with OAs from Ireland. Our six-step research process used to explore mobile phone usage of OAs is explained in the sidebar. The next section sheds light on how OAs use their mobile devices.

Results

The ratio of participants in our sample is 60/40 for females and males and most fall between the ages of 60 to 70. Figure 1 depicts the smoothed kernel density estimation (KDE) curves that estimate the distribution of hours per week spent by OAs on using mobile phones. If someone reported a range – e.g., "4 to 6 hours" – their vote is scaled down and evenly distributed over that time range. We used three independent variables to check their correlation with mobile phone adoption - residence, education and living arrangements. Interestingly, OAs without a qualification spent less time each week using a mobile phone compared with someone possessing any level of schooling or degree. The majority of the OAs spend 0 to 2 hours on their mobile phones, while the number of OAs using the mobile phone for 4-6 hours is less. The number of OAs spending 8 to 10 hours on their mobile device increases, as depicted in Figure 1. Interestingly, we also note that this increase is irrespective of the education level. This leads us to infer that there are two main categories of OAs: – those who use mobile phones minimally for communication, and those whose mobile phones are an integral part of their lives. One unexpected finding was that younger OAs living in rural areas are using mobile phones more in comparison with those younger OAs living in cities. This could be due to the lack of physical access to other people in towns. In addition, people living with extended families are spending significantly longer amounts of time on mobile devices when compared with other groups. As shown in Figure 3, OAs in our sample are using android-based mobile devices more than any other type of mobile phone. In addition, Figure 4 reveals the top mobile phone activities which OAs of different ages perform are: calling, texting, group chatting, sharing photos and videos and managing daily activities. The majority (76%) of OAs have access to the internet on their mobile devices, which is helpful when using wearable technology such as keeping track of OAs' activities. But, there are still very few OAs (Figure 2) who are familiar with wearables such as Fitbit. To understand why and the implications of this, we need to follow this up with further research. The positive view of this is that 61% of OAs have shown interest in such devices. We also asked OAs about any additional comments which they would like to make about our mobile-based system

3. Collect Data: The survey was conducted online using Google Forms which is open source, free and supports automatic collation of data in a spreadsheet. The questionnaire had 13 demographic questions, and 17 survey questions. 202 completed questionnaires were returned.

4. Code Data: Qualitative responses to open questions were coded to create themes in respect of our variables studies (e.g. likes, dislikes). The coding was conducted manually, and two researchers were involved.

5. Analyze Data: The quantitative results (Likert scale responses), were aggregated in Microsoft Excel. We aggregated the demographic responses to gain a picture of our sample.

6. Report Results: The results are reported using both descriptive and inferential statistics based on the research question.

which we are developing. They understood its importance and expressed an interest in this. But, they highlighted privacy as their primary concern even without prompting, as indicated in the literature [2]. An OA said *"I'd have privacy concerns about an app that went deep into health and fitness!"*

Discussion

The findings of this survey will help practitioners develop effective mobile-based applications for OAs. They need to incorporate the most liked features by OAs such as information-seeking and communication along with the key non-functional requirement, privacy. This is in line with literature [2, 13, 18], which states privacy concerns of OAs relating to mobile devices as: constant monitoring, collection and dissemination of private information, proliferation of unregulated apps in the market and lack of self-efficacy of OAs to use these devices. Currently, the wearables and devices deployed in OA homes gives them a sense of continuous monitoring and can cause distress and resistance to use. This can be addressed by making these devices work for a fixed duration and location where OAs are comfortable. The license agreement should be short and written in clear language informing OAs about how their data will be used, instead of the current format which is long and complex. Unregulated apps are the biggest threats to data breach, which can be resolved by providing OAs with information and devising new standards. One to one sessions should be conducted with OAs as well to enhance their self-efficacy, so that they manage their privacy on their own whilst using mobile devices. The inherent heterogeneity of this age group also needs attention whilst developing any kind of system for them. Also, as a start, android platforms should be considered as they are inexpensive and widespread as indicated by our cohort. In our project, we are following these findings to develop an exemplar mobile-based social networking system that suggests volunteer opportunities to OAs within the community. The objective is to keep people connected with communities and avoid problems of social isolation by using this form of technology as a mediator.

To mitigate external validity, we used a convenience sampling approach i.e. participants are from Ireland, have access to the internet, already familiar with technology and are interested in volunteering. So, the results are not generalizable for the whole OA population. Similarly, to mitigate internal validity, the majority of the questions helped us extract the intended information, even though, some OAs weren't able to understand some questions.

Conclusion

This study revealed the current practices, preferences and expectations of OAs from mobile devices especially mobile phones and wearables. Several inferences were also made concerning mobile phone usage based on variables such as education, residence and living arrangements. In conclusion, a vast majority of OAs possess mobile devices with data plan. They are willing to use new applications and systems if they are designed for and with them by ensuring privacy.

Acknowledgements

This work was supported, in part, by Science Foundation Ireland grant no. 13/RC/2094, IBM Damastown Campus Dublin, Ireland & Ireland Smart Ageing Exchange.

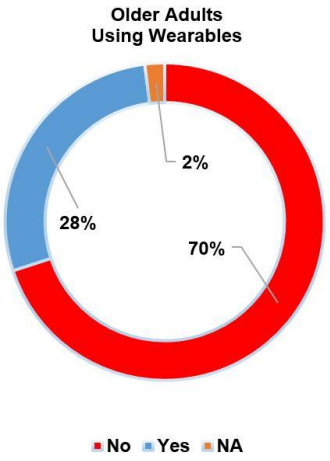


Figure 2: Percentage of older adults using wearables like Fitbit

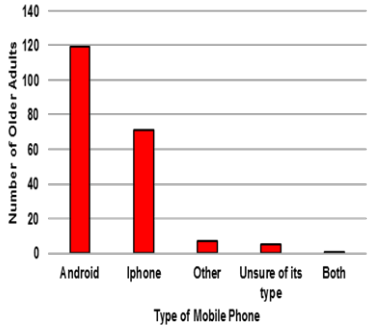


Figure 3: Type of mobile phone used by older adults

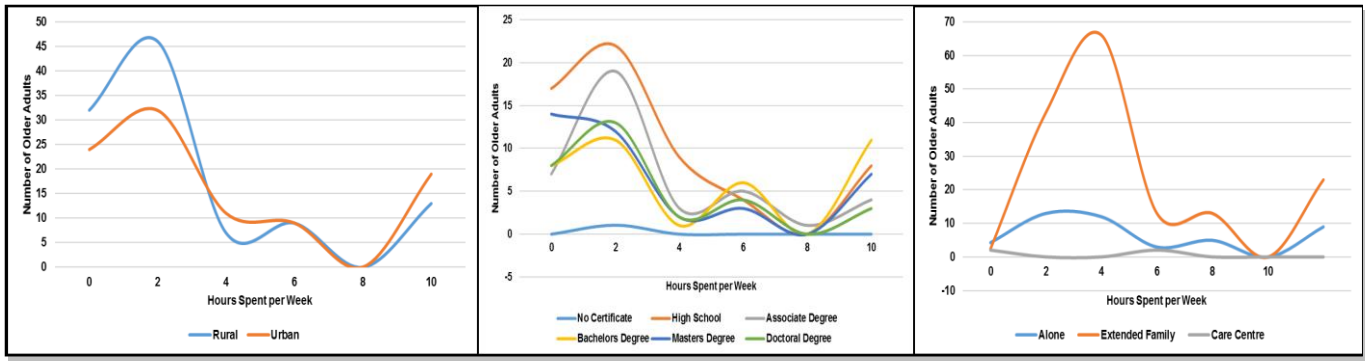


Figure 1: Correlation of residence, education and living arrangements with mobile phone adoption

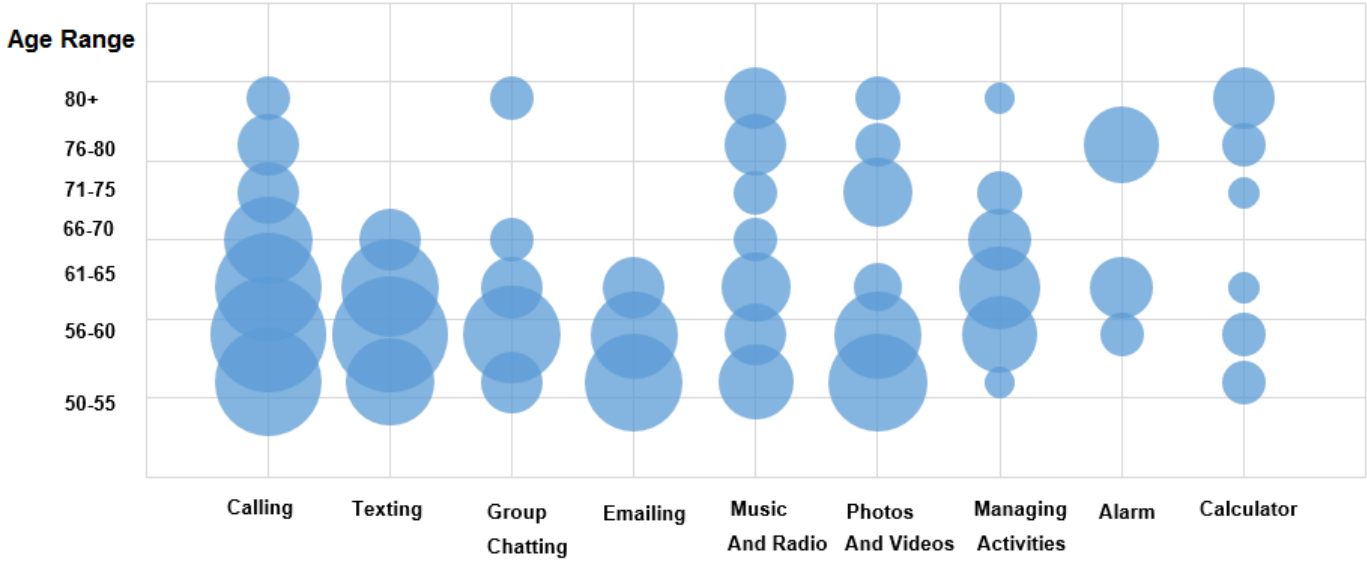


Figure 4: Frequency of top mobile phone activities by older adults of different ages

References

1. Ageing Well Network 2012. The New Agenda on Ageing: To Make Ireland the Best Country to Grow Old In.
2. Ahmad, B., Richardson, I. and Beecham, S. 2017. A Systematic Literature Review of Social Network Systems for Older Adults. Product-Focused Software Process Improvement. Springer International Publishing. 482–496.
3. Arreola, I., Morris, Z., Francisco, M., Connelly, K., Caine, K. and White, G. 2014. From Checking on to Checking in. Proceedings of 32nd ACM conference on Human factors in computing systems.
4. Brunette, K., Eisenstadt, M., Pukinskis, E. and Ryan, W. 2005. Meeteetse: Social Well-being through Place Attachment. CHI '05 extended abstracts on Human factors in computing systems.
5. Burmeister, O. 2012. What Seniors Value About Online Community. The Journal of Community Informatics. 8, 1 (Feb. 2012).
6. Chen, K., Chan, A.H. and Tsang, S.N. 2013. Usage of Mobile Phones Amongst Elderly People in Hong Kong. The 2013 IAENG International Conference on Industrial Engineering Special Session: Human Factors, Ergonomics, and Safety.
7. Guo, P.J. 2017. Older Adults Learning Computer Programming. Proceedings of 2017 CHI Conference on Human Factors in Computing Systems.
8. Hope, A., Schwaba, T. and Piper, A.M. 2014. Understanding Digital and Material Social Communications for Older Adults. Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI '14 (2014).
9. http://www.cso.ie/en/csolatestnews/pressreleases/2017pressreleases/pressstatementcensus2016resultsprofile3-anageprofileofireland/. Accessed: 2018-06- 20.
10. Latulipe, C., Gatto, A., Nguyen, H.T., Miller, D.P., Quandt, S.A., Bertoni, A.G., Smith, A. and Arcury, T.A. 2015. Design Considerations for Patient Portal Adoption by Low-Income, Older Adults. Proceedings of ACM Conference on Human Factors in Computing Systems.
11. Leung, R., Tang, C., Haddad, S., Mcgrenere, J., Graf, P. and Ingriany, V. 2012. How Older Adults Learn to Use Mobile Devices. ACM Transactions on Accessible Computing. 4, 3 (Dec. 2012), 1–33.
12. Mohadisdudis, H.M. and Ali, N.M. 2014. A Study of Smartphone Usage and Barriers Among the Elderly. 2014 3rd International Conference on User Science and Engineering (i-USEr) (Sep. 2014).
13. Nef, T., Ganea, R.L., Müri, R.M. and Mosimann, U.P. 2013. Social Networking Sites and Older Users – A Systematic Review. International Psychogeriatrics. 25, 7 (Apr. 2013), 1041–1053.
14. Plaza, I., Martín, L., Martin, S. and Medrano, C. 2011. Mobile Applications in an Aging Society: Status and trends. Journal of Systems and Software. 84, 11 (Nov. 2011), 1977–1988.
15. United Nations 2002. World Population Ageing: 1950-2050. Department of Economic and Social Affairs.
16. Van Tilburg, T. 1998. Losing and Gaining in Old Age: Changes in Personal Network Size and Social Support in a Four-Year Longitudinal Study. The Journals of Gerontology: Psychological Sciences and Social Sciences. 53B, S313–S323.
17. World Health Organization 2014. Definition of an Older or Elderly person. http://www.who.int/healthinfo/survey/ageingdefnolder/en/index.html
18. Xie, B., Watkins, I., Golbeck, J. and Huang, M. 2012. Understanding and Changing Older Adults' Perceptions and Learning of Social Media. Educational Gerontology. 38, 4 (Apr. 2012), 282–296.

I'm Not That Old Yet! The Elderly and Us in HCI and Assistive Technology

Lothar Fritsch
Karlstad University
65188 Karlstad, Sweden
Lothar.Fritsch@kau.se

Ingvar Tjøstheim
Norwegian Computing Center
0314 Oslo, Norway
Ingvar.Tjostheim@nr.no

Agnieszka Kitkowska
Karlstad University
65188 Karlstad, Sweden
agnieszka.kitkowska@kau.se

In: Proceedings of the Mobile Privacy and Security for an Ageing Population workshop at the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI) 2018, Barcelona

Abstract
Recent HCI research in information security and privacy focuses on the Elderly. It aims at the provision of inclusive, Elderly-friendly interfaces for security and data protection features. Much attention is put on care situations where the image of the Elderly is that of sick or disabled persons not mastering contemporary information technology. That population is however a fraction of the group called the Elderly. In this position paper, we argue that the Elderly are a very diverse population. We discuss issues rising from researchers and software architects' misconception of the Elderly as technology-illiterate and unable. We suggest a more nuanced approach that includes changing personal abilities over the course of life.

Author Keywords
e-Inclusion, HCI, information security, information privacy, data protection, usability, elderly

ACM Classification Keywords
• **Human-centered computing~User models** • Human-centered computing~Accessibility theory, concepts and paradigms • **Software and its engineer-**

Expect the Young when designing for the Elderly!

Look ahead into the demography: Consider today's middle and younger generations' skills that will flow up into the Elderly group! While personal abilities may decline with age, the Elderly as a group will have increasing technology mastership!

Inclusiveness, not special-needs: Design your applications in ways that present the same functionality for the Elderly as for the young populations! Restricted functionality and oversimplified ideas of capabilities frustrated the Elderly.

Anticipate broad diversity in abilities and skills: Do not focus on missing abilities or disabilities in the Elderly, but anticipate a broad variety of abilities that can change over time.

ing~Software usability • Security and privacy~Social aspects of security and privacy • Security and privacy~Usability in security and privacy

Introduction

Human life evolves in phases with varying abilities, skills and limitations. Being Elderly is not a function of age and an assumption about consequences of old age. We argue that the Elderly as diverse in their abilities, needs and skills as any other group of society. Abilities evolve and decay at individual rates. These abilities depend on personal histories and education. Personal health is an individual determinant. Cultural influences and expectations place the Elderly in roles. Strategies to cope with age-induced limitations are diverse and individual, while age-related paternalism may force the Elderly into imposed roles that impair abilities. In addition, interaction goals change over time. Life transitions may influence the purpose and way that technology is used by the elderly. Elderly may use the same technology for different purpose, i.e. applications previously used for work now get used to connect. Attitudes to information security and information privacy needs are diversified through age, background and experience. Older generations have negative views on digital information disclosure, they seem to be more concerned; perceive privacy risks as more difficult to prevent [5].

Concepts of the Elderly in HCI

The concept of the Elderly is ill-defined in literature and research projects. There is no static age for becoming an Elder. While reaching pension age is one often-used indicator, other sources claim around 50 years of age [6]. Sometimes, as in *elderly statesman*, the connotation is positive, but this seems to be an exception. In 1995, the elderly workforce was in need of computer education and was described as challenged by learning to use computers [2]. Elderly users are generally described as a group with age-related impairments compared to a younger norm population. Impairments concern vision, physiology, hearing and cognition[1]. We can observe this in research that we have been involved [8]. The Elderly are depicted as being disinterested in technology – persona Paul Clason's attitude being constructed as: "I'm too old to learn how to deal with all these tools." [8]. Project MECS at Oslo University seems to define the Elderly as "dynamic obstacles" from the perspective of a care robot[2]. In e-health, the Elderly are the group from age 50: "The group is said to show less perception and control capability and has less experience in the use of information technology. More realistically, the group of 50+ users shows more diversity in their cognitive, sensory and motor skills than younger people." [3]. In project e-Me [7], research looked into alternative authentication methods. It produced prototypes of various graphical and audio-visual methods. The test panel was staffed with volunteers from Norway's association of the Elderly. One prototype was a matrix with animal pictograms with their respective sounds. Replacing a password by a self-chosen sequence of animal pictograms and sounds, the prototype aimed at helping recall password sequences. The Elderly response to this particular prototype was not enthusiastic: *"Please note that we are grown-ups!"*

[1] ,W3C Web Accessibility Initiative, Older Users and Web Accessibility:Meeting the Needs of Ageing Web Users, http://www.w3.org/WAI/older-users/ , 2018-05-14

[2] Project Multimodal Elderly Care Systems (MECS), http://www.mn.uio.no/ifi/english/research/projects/mecs/index.html, 2018-05-11

This should motivate a nuanced and more sensitive approach to this type of research.

Perspectives on age and ability

Young today, Elderly tomorrow: Fluctuation of skills and technology attitudes within a decade or two must be expected (see **Figure 1**). A survey of privacy attitudes showed that the younger smartphone users were not more aware of smartphone privacy settings than the older ones, with the results indicating that such awareness is, or can be created in adolescence and then persists through life [9]. We can learn at all ages. Education and motivation can have an impact or determine individual abilities and technology-fluency strongly. Other influence factors are expected cultural roles for the Elderly. We have observed that some elderly seem to have a strong aversion against being made "look old" because they are offered assistive technology or technology for Elderly[1].

A major concern is surveillance. Age-related paternalism might force the Elderly into the use of surveillance services. Do elderly understand the risks of such monitoring? Do they agree or disagree to be tracked? This may affect between-generations relations, or mental states of elderly users. Technologies such as GPS-based tracking or mobile control and feedback for exercise or diet may impose societal norms beyond the individual's wishes, turning health of the Elderly into surveillance [4].

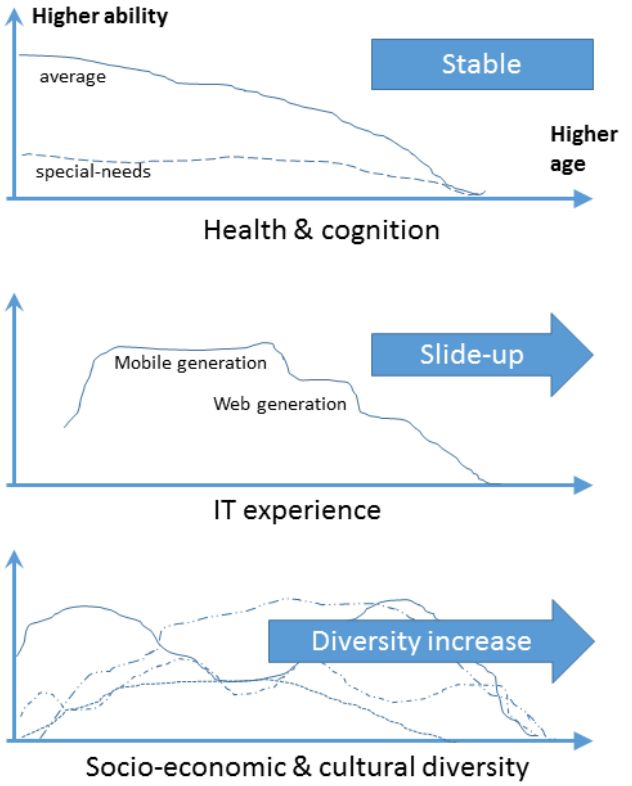


Figure 1: Dynamic abilities come from new generation's abilities that flow up the time line. In addition, a more diverse society will meet a more diversified elderly population. This is of particular relevance in societies with social, economic and educative differentiation and immigration.

A diversified image of ageing populations

We suggest the dissolution of the Elderly as the group of incapable old people, and propose a diversified model based on skills and other parameters. The traditional model of the Elderly as less capable humans who – for their declining abilities – need to settle for simpler

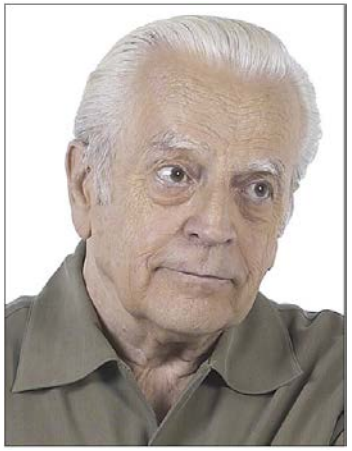


Figure 2 "**I'm too old to learn how to deal with all these tools**."
Typical Elderly persona called Paul Clasen as defined by research project uTrustIT: 75 years old, dementia issues, [8].

solutions is not appropriate. When a personas technique is used, we should keep this in mind. We suggest a dynamic matrix with descriptive abilities that would lead to a family of personas for a varied population of the Elderly. This concept neatly reaches into and gains insight from younger populations such as in the ALerT project [9]. We are convinced that certain capabilities – such as technology fluency – move up with age with the generations. For test and user studies, we should recruit a diverse user group with a wide spectrum of abilities in the group of the Elderly. As has been pointed out for authentication and identity management technology in earlier studies [1], a multi-modal approach with many ways to solve issues will be preferable over a single one-size-fits all model of the Elderly.

Conclusion

Designing for the Elderly should anticipate the skills and expectations of the diverse not-so-elderly as the coming users of the systems rather than defining the Elderly as a subset of a norm set of average population abilities.

Acknowledgements

Supported by the ALerT project, Research Council of Norway, IKTPLUSS 2017-2021 and from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675730 Privacy&Us.

References

1. Lothar Fritsch, Kristin Skeide Fuglerud and Ivar Solheim. 2010. Towards Inclusive Identity Management. Identity in the Information Society, 3 (3). 515-538. 10.1007/s12394-010-0075-6 Open Access
2. Catherine L Kelley and Neil Charness. 1995. Issues in training older adults to use computers. Behaviour & Information Technology, 14 (2). 107-120.
3. Andreas Lorenz and Reinhard Oppermann. 2009. Mobile health monitoring for the elderly: Designing for diversity. Pervasive and Mobile Computing, 5 (5). 478-495.
4. Deborah Lupton. 2012. M-health and health promotion: The digital cyborg and surveillance society. Social Theory & Health, 10 (3). 229-244. 10.1057/sth.2012.6
5. Caroline Lancelot Miltgen and Dominique Peyrat-Guillard. 2014. Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. European Journal of Information Systems, 23 (2). 103-125.
6. Fariza Hanis Abdul Razak, Rafidah Sulo and Wan Adilah Wan Adnan. 2012. Elderly mental model of reminder system Proceedings of the 10th asia pacific conference on Computer human interaction, ACM, Matsue-city, Shimane, Japan, 193-200.
7. Till Halbach Røssvoll and Lothar Fritsch. 2013. Trustworthy and inclusive identity management for applications in social media. Kurosu, M. ed. Human-Computer Interaction. Users and Contexts of Use - International Conference on Human-Computer Interaction HCI 2013, Springer, 68-77.
8. Trenton Schulz, Cornelia Graf, Christina Hochleitner and Kristin Skeide Fuglerud. 2011. D.2.1 Personas Deliverable of the uTRUSTit project, Norwegian Computing Center, 1-20.
9. Ingvar Tjøstheim et al. 2017. Awareness Learning Tools for Data-sharing Everywhere NR Note, Norsk Regnesentral, Oslo, Norway.

Similar Information Privacy Behavior in 60-65s vs. 50-59ers - Findings From A European Survey on The Elderly.

Tjostheim, Ingvar
Norwegian Computing Center
Blindern, 0314 Oslo, Norway
ingvar@nr.no

Fritsch, Lothar
Karlstad University,
651 88 Karlstad
lothar.fritsch@kau.se

Abstract
In this article, we present findings from a European survey with 10 countries on the subject sharing of personal information and concerns of the citizens. We compare the age group 60-65 years old with the age group 50-59, and in addition compare the Nordic region with the non-nordic population. There are more similarities than differences. The survey indicates that many of the elderly 60-65 take steps to protect their personal data.

CONF '22, Jan 1 - Dec 31 2022, Authorberg.

unique doi string will go here

Author Keywords
Information privacy; elderly; sharing of personal data; privacy-concerns.

ACM Classification Keywords
• Security and privacy ~Social aspects of security and privacy • Information interfaces and presentation

Introduction
Data is the fuel of the digital economy, but data about us individuals also represents problems and challenges of relevance for privacy, transparency and digital literacy. Since Westin's book Privacy and Freedom [6], many studies have used a segmentation model
that divides consumers into three classes based on thei r privacy preferences: fundamentalists, pragmatists, an d the unconcerned. One example is the privacy seg-

mentation index that consists of three questions and a set of rules to translate participants' responses into these three categories was developed. However, there are some limitations to these kinds of studies [3] [6].

What people state in a survey is not necessarily highly correlated to what they actually do. The privacy paradox is the phenomenon where an individual expresses privacy concerns but behaves in a contradictory way to these concerns [2]. Reasons for this mismatch between attitude and stated preferences are well documented in the literature on choice behavior. Sometimes people are satisficing and give social acceptable answers. We also know that people do not always make choices in accordance with their own self-interests. Still, surveys can give an indication of citizens' attitudes and behavior. Given that the statements and survey question have relevance, are easy to understand, and not vague or difficult, it is a valuable source of information.

Method and profile of the participants.

To get knowledge about sharing of personal data and what citizens perceive as problematic, we conducted a web-based survey targeting online and mobile phone users aged 16 to 65. We build on the report *Europeans' attitudes towards cyber security (2017)* and a survey on digital services by the Norwegian Consumer Council in 2015 [8]. The EU-study is based on personal interviews with 22.236 respondents (Internet users), representing 340 million Europeans in 28 EU countries. The Norwegian survey had 960 participants recruited from a web panel.

In 2017, the Norwegian Research Council funded project *Awareness Learning Tools for Data Sharing Everywhere* (ALerT). One questions relevant for ALerT-project is citizens' experience with sharing personal data, and concerns about misuse of such data. The survey reported in this paper is the *ALerT survey*. The ALerT- and the cyber-security surveys are not directly comparable due to different sampling methods, but they were carried out in the same period, June to September 2017.

1605 participated in the survey carried out by Polling & Statistics AS. The fact that a person has accepted an invitation to be included in a panel run by a market research company indicate that the person has at least basic ICT-skills. The panel-member receives emails with a link to a web-based survey – there is no obligation to respond and participate in all surveys, but a hypothesis is that the somewhat more active individuals with opinions tend to participate. This means that the findings should not be interpreted as representing the average view in a national population. One should not expect the privacy fundamentalists as members of such groups. A stratified sampling technique was used on the variables gender (approx. 50/50), age and regions in the country. Since we are particularly interested in age, we present the age-profile of the 1605 participants in Table 1.

Age groups:	16-29	30-49	50-59	60-65
Four Nordic Countries	466	213	105	62
Six European Count.	255	275	153	76
Total (N)	721	488	258	138

Table 1: Age profile of respondents.

Next, we compare the 60-65 group to the 50-59ers for the four Nordic countries and for the six other European countries. We performed a Pearson chi-square test

What are the differences between 60-65s and 50-59ers?

Findings
The answers to the general questions indicate the citizens that participated in the survey have good knowledge and know how to protect their personal data.

When the citizens are asked about their behavior, what they do to control sharing of data, the percentages are lower. For the other questions, for the 60-65, it is approximately 50 percent yes/no or agree/disagree answers indicating a greater variety in attitudes and behavior.

The main finding is that the elderly 60-65 are similar to the 50-59, although some differences are identified.

Countries (ALerT-survey)
Norway, Sweden, Denmark, Finland, Germany, UK, the Netherlands, France, Italy and Poland

between the two groups; p< .1 is * and P<.05 is **. Table 2 shows the result.

Questions asked

The first section of the survey had the following four questions;

1. *"Consider your computer or Internet skills. Do you know how to protect your personal data?* "
2. *"Consider your computer or Internet skills, do you know how to protect your private computer from virus or other computer infections?"*
3. *"Have you changed the privacy setting in your Internet–browser or in an app to avoid sharing of personal data?"*
4. *"App on your smartphone, have you restricted or refused access to your personal data (e.g. your location, contact list)?"*

The answers are self-reports, thus not an accurate description of behavior. Still, we might assume that the participants have knowledge about their behavior. The answers give indications about behavior, and reveal differences if any between the age groups. We are particularly interested in the 60-65 vs. the 50–59 group.

Age groups:	16-29	30-49	50-59	60-65
Four Nordic C. Yes, I know how to protect p. data	72%	76%	79%	66%*
Six European C. Yes, I know how to protect p. data	88%	90%	87%	84%

Table 2: For the Nordic group the percentage that answers yes I know how to protect my personal data is significantly lower (p<0.1) for the age group 60–65 vs. 50-59.

For the question *have you changed the privacy settings* and the question *have you restricted or refused access to personal data when installing or using an app*, only one difference is identified (P<.05). The answers indicate a significant difference for the six European countries for the 60-65 vs. the 50-59 on the question restricting access (see Table 3).

Age groups:	16-29	30-49	50-59	60-65
Four Nordic C. *changed* settings Yes, more than once	50%	63%	54%	45%
Six European C. changed settings Yes, more than once	44%	46%	41%	42%
Four Nordic C. ..restricted access.. Yes, at least once	73%	70%	53%	50%
Six European C. ..restricted access .. Yes, at least once	81%	78%	61%	49%**

Table 3: Use of privacy settings (age/region).

The next question concerns choices against smartphone apps when they require access to personal information. The questionnaire item is *"Have you decided not to download an app on your mobile phone because the app required personal information that you did not want to share (example: your contact list)."*

Age groups:	16-29	30-49	50-59	60-65
Four Nordic Count. I have decide not to download an app… Yes, more than once	42%	63%	58%	58%

Six European C.				
I have decide not to download an app…				
Yes, more than once	45%	60%	58%	59%

Table 4: The answers indicate no differences - the age groups 60-65 answers and the group 50-59 answers are similar.

The last question concerns sharing of contact lists. Its purpose is to elicit the positive or negative attitude to sharing without consent. This question might indicate whether a person reflects on and is concerned about privacy. The fact that someone on a contact list is not asked is one of the more privacy-intrusive practices in today's digital environment [7]. *"An app-provider should be allowed to use your contact-list also for other purposes than the app needs to function*." Table 5 shows the results for the alternative fully disagree.

Concluding remarks

There are differences between age groups, but there is no clear pattern indicating the 60-65s should be significantly different from the 50-59ers in the sense that they are less concerned, less willing to protect data and/or less able to control sharing of personal data. Taken together, there are more similarities than differences between both age groups. The group of the Elderly in their 60ies does show ICT awareness and privacy attitudes similar to the population a decade younger. One may expect the group of the ICT-illiterate high-age Elderly to shrink over time.

Age groups:	16-29	30-49	50-59	60-65
Four Nordic C.				
use of contact-lists				
Fully disagree	53%	63%	65%	68%

Six European C.				
use of contact-lists				
Fully disagree	44%	62%	57%	57%

Table 5: Sharing of contact lists (age/region).

References

1. European Union 2017. 5661. Special Eurobarometer 464a "European attitudes towards cyber security", September 2017
2. Paul A. Pavlou. 2011. "State of the Information Privacy Literature: Where We Are Now and Where We Should Go?" MIS Quarterly, 35 (4), 977-988
3. Ponnurangam Kumaraguru, Lorrie Faith Cranor. 2005. Privacy Indexes: A Survey of Westin's Studies. Working Paper CMU-ISRI-5-138, Carnegie Mellon University
4. Ingvar Tjøstheim et al. 2017. Awareness Learning Tools for Data-sharing Everywhere NR Note, Norsk Regnesentral, Oslo, Norway.
5. Alan F. Westin. 1967. Privacy and Freedom, New York: Atheneum.
6. Allison Woodruff, Pihur, V., Conslove, S., Brandimarte, L., and A. Acquisti, 2014. Would a privacy fundamentalist sell their DNA for $1000...if nothing bad happened as a result? The Westin categories, behavioral intentions, and consequences. In Proceedings of the 2014 Symposium on Usable Privacy and Security (2014), USENIX Association, pp. 1–18.
7. Lothar Fritsch, 2017. Privacy dark patterns in identity management. In LNI (277), Proceedins of Open Identity Summit (OID) 2017, GI Edition Bonn, 93-104. ISBN 978-3-88579-671-8
8. Norwegian Consumer Council: Population survey; June 2015, https://fil.forbrukerradet.no/wp-content/uploads/2016/01/Rapport_apper.pdf

Seniors' Media Preference for Receiving Internet Security Information: A Pilot Study

Yousra Javed
Illinois State University
yjaved@ilstu.edu

Mohamed Shehab
University of North Carolina
Charlotte
mshehab@uncc.edu

Boyd Davis
University of North Carolina
Charlotte
bdavis@uncc.edu

Abstract

Due to the increasing use of Internet by older adults and their low computer and Internet security literacy, their susceptibility to online fraud has also increased. This suggests in turn that there are still too few Internet education materials targeting seniors. We take a first step towards developing interactive security information materials for seniors by determining which media they prefer and can easily comprehend. We studied the reception of two media, text and audio, as they communicated information about email-based phishing attacks. Our preliminary study of 34 seniors shows that the participants personally preferred the text over the audio. However, the comprehension score was not significantly different for participants who read the phishing text script as compared to the participants who listened to the phishing audio script.

Introduction

The Pew Research Center reported in 2014 on the ever-increasing number of senior citizens moving to use the Internet. Safety and security are primary objectives for the growing number of seniors using the Internet: currently, 59% of seniors over 65 use the Internet [6] and, given that seniors are the fastest growing demographic, this cohort should increase annually. But online seniors are vulnerable seniors. Researchers identify user concerns about areas such as website disclosure about purchasing history,

browsing patterns or personally identifiable information, and scams, phishing and malware, and financial scams [3]. Seniors are apparently highly vulnerable as many have low computer literacy, low awareness of Internet pitfalls, and even less knowledge about where to find information about Internet security.

Existing HCI research mostly focuses on younger adults and university students, and rarely includes participants aged 60 and above [4]. Many factors contribute towards this. First, older adults are an extremely diverse group. They have significantly different lifestyle characteristics from the younger adults since most of them live far from universities. In addition, aging causes sensory changes such as visual and auditory perception, and cognitive changes such as working memory. Thus, they are more likely to forget instructions and take longer to reach a level of proficiency. Various mobility issues and illnesses may exist in older people that make it difficult for them to participate in research studies. Secondly, due to these inherent characteristics of older adults, important considerations need to be incorporated in the experimental design in order to get high quality results from them. For example, the use of flexible timing, cognitive testing, and instructions for getting to the research study venue all need to be built into the design. Thirdly, appropriate recruitment methods need to be employed in order to ensure access to a useful sample of older people.

In order to develop interactive materials related to Internet security for seniors, it is important to first determine the seniors' media preferences. However, to the best of our knowledge, there is no existing study that explores seniors' media preference for receiving training involving computer and Internet security information, and their comprehension of each medium.

We conducted a pilot study on seniors' media preference for receiving computer and Internet security information. We focused on two media types: print text and audio, and designed scripts to communicate information about email-based phishing, and tips they can use to protect themselves against such scams. We chose email-based phishing, since it is one of the main tools used for financial fraud. Accordingly, our study focused on answering the following research questions:
1. Which of the two media types results in better comprehension of email-based phishing?
2. Which of the two media types do seniors prefer?

Study Design

Our study, approved by the UNCC Institutional Review Board[1], followed a between-subjects design. The two treatment conditions were:
Treatment 1 - Text: The participants read the text script on email-based phishing.
Treatment 2 - Audio: The participants listened to an audio script on email-based phishing. The audio script was a screencast/voice-over the text script and had essentially the same contents as the text script.

After reading/listening to the script, the participants completed a phishing comprehension survey. After completing the survey, the participants were required to listen to/read the other media script for the purpose of providing their media preference and rating of the provided scripts. The number of male and female participants in each treatment group was controlled for.

Surveys

Phishing comprehension
The phishing comprehension survey consisted of a total of 10 questions. The first five questions asked the participants

[1] Approved IRB Protocol#14-04-11

to label each shown email message as a legitimate or a phishing email. The next five questions were designed to test other information provided in the text and audio scripts. Based on the responses, a score was computed out of 10.

Media preference and rating
The participants answered the following questions:
Q1. Rate the audio message (Likert scale: 1 - 5)
Q2. Rate the text message (Likert scale: 1 - 5)

Demographics
The demographics survey comprised of 10 questions to analyze the characteristics of our participant pool.

Participants

Initially, we planned on recruiting our participants from senior centers situated off-campus, by posting flyers on their websites [1, 2]. 10 seniors contacted us and showed interest in participation. However, only two of them actually participated in the study.

The following factors impeded our recruitment process:
1. Reposting the flyers did not increase the number of seniors who responded to our flyers.
2. Most of the seniors who showed an initial interest in the study could not participate later on due to health issues or personal commitments.
3. A few senior centers did not give us direct permission to visit the seniors in the computer class at the senior center and interview them. Therefore, they kept us waiting for response from their senior managers.

Due to the difficulties we experienced while recruiting participants from the senior centers, we recruited our participants from Amazon Mechanical Turk (a crowdsourcing marketplace). We set up our study as a Human Intelligent Task (HIT), which included the tasks described in Section .

Due to the fact that a small percentage of older adults uses Amazon Mechanical Turk, we reduced the minimum eligible from 65 to 55. To ensure that only the people aged 55 and above attempt the survey, we set up our demographic survey as an eligibility screening survey. Only the participants who selected 55 and older as their age group in the demographic survey were asked to proceed with the HIT. To better control the quality of the recruited participants, we mandated that each worker has a 90% HIT approval rating, or better. The HIT took approximately 30-40 minutes to complete, for which each worker was paid a fee of $1. A total of 34 participants (17 per group) successfully completed the pilot study.

Results

Phishing Comprehension (Text script vs Audio script)
An overall comprehension score was calculated based on the number of phishing related questions that were answered correctly (out of 10). We conducted the Wilcoxon-Mann Whitney test on the phishing comprehension scores of the two treatment groups. The test showed no significant difference between the phishing comprehension score of the text script (μ=7.3, σ=1.57) and the audio script (μ=8.29, σ=1.96) with p= 0.07.

Media Preference
Chi-squared test was conducted between the media preference for the two participant groups. The test showed that both groups have similar media preference since the p value was greater than 0.05. Both groups preferred the text media over the audio–70.5% participants in the first group, and 64.7% participants in the second group. We also conducted a Wilcoxon signed-rank test between the overall Likert scale ratings of both messages. The test showed no significant differences in the ratings for text (μ=3.9, σ=1.19) and audio (μ=3.7, σ=1.13) message with p=0.44.

Related Work

Garg et al. [5] studied the effectiveness of narrative-driven videos vs text for communicating phishing and malware email-based online risk to older adults. Their pilot study on 12 participants showed that video helped the participants in verbalizing the risk of responding or not responding to the emails. However, both the video and text made the participants rate the risk of responding to emails higher than that of not responding to them.

Conclusion and Implications

Our pilot study on seniors' media preferences for instructional material suggests that Dickinson's findings regarding seniors' recruitment still hold true. Dickinson states that issues such as illness and family responsibilities make it hard to recruit and schedule sessions with the seniors. Most of the seniors who initially showed interest in our study, could not participate later for similar reasons. We hoped to get a large turnout from the senior centers. In future, we plan to work with local charities and offer free computer classes (in exchange for participation) as suggested by Dickinson.

People use the Internet for interpersonal reasons, to pass time, seek information and be entertained; MAIN, a new model for technology affordances, suggests that the visual component of multimedia surpasses text in terms of informational content delivery; however, a visual can also be seen as a distractor [7]. New models of technology usability and gratification often lack focus on the newly emerging audience of seniors. We originally hypothesized that the empirical findings of our pilot would be able to support theoretical exploration of media acceptance by seniors and thereby enable us to tailor expanded interactive materials about security to their preferences. However, the barriers we encountered in recruiting seniors suggest that we need to develop alternative ways to recruit participants before seeking funding. Accordingly, we have revised our recruiting to include families with members placed into adult day care and caregivers for homebound cognitively impaired seniors, to develop materials and identify preferences for our VA-funded project, StoryCall, and are considering targeting churches which, particularly for minorities, often present health and computer education for its parishioners.

REFERENCES

1. 2018. Charlotte Mecklenburg Senior Centers. (2018). `https://www.mecknc.gov/ParkandRec/Facilities/Pages/Senior-Centers.aspx`.
2. 2018. The Laurels At Highland Creek. (2018). `https://www.fivestarseniorliving.com/communities/nc/charlotte/the-laurels-the-haven-in-highland-creek`.
3. Martha Deevy, Shoshana Lucich, and Michaela Beals. 2012. Scams, schemes & swindles. *Financial Fraud Research Center* (2012).
4. Anna Dickinson, John Arnott, and Suzanne Prior. 2007. Methods for human–computer interaction research with older people. *Behaviour & Information Technology* 26, 4 (2007), 343–352.
5. Vaibhav Garg, L Jean Camp, Katherine Connelly, and Lesa Lorenzen-Huber. 2012. Risk communication design: Video vs. text. In *International Symposium on Privacy Enhancing Technologies Symposium*. Springer, 279–298.
6. Aaron Smith. 2014. *Older adults and technology use*. Pew Research Center.
7. S Shyam Sundar and Anthony M Limperos. 2013. Uses and grats 2.0: New gratifications for new media. *Journal of Broadcasting & Electronic Media* 57, 4 (2013), 504–525.

Appendix

Participant Demographics

Demographics		*No. of Participants*
Education	High School 2 years of college 4 years of college $>$ 4 years of college	3 8 11 12
Social media use	Facebook Twitter LinkedIn None	24 5 1 4
Are you concerned about security and privacy when using the Internet	Yes No	29 5
Which device are you using to complete this survey	Laptop PC Smartphone	19 14 1
How long have you been using the Internet	Less than 5 years More than 5 years	6 28
Number of times you have been a victim of Internet attack/scam	0 1 More than 1	12 9 13

Table 1: Participant Demographics

Scripts for Education on Email-Based Phishing

Text script link: https://goo.gl/noeybq
Audio script link: https://goo.gl/6oj86n

Surveys

Phishing Comprehension: https://goo.gl/Y4Tdc3
Media Preference: https://goo.gl/GfSfkX

Demographics		*No. of participants (Text Script Group)*	*No. of participants (Audio Script Group)*
Gender	Female Male	11 6	8 9

Table 2: Participant distribution within groups

“Outsourcing” Security: Supporting People to Support Older Adults

Lukas Mecke
Munich University of Applied Sciences, Germany
lukas.mecke@hm.edu

Mohamed Khamis
University of Glasgow, Scotland
LMU Munich, Germany
mohamed.khamis@ifi.lmu.de

Sarah Prange
Munich University of Applied Sciences, Germany
sarah.prange@hm.edu

Mariam Hassib
LMU Munich, Germany
mariam.hassib@ifi.lmu.de

Daniel Buschek
LMU Munich, Germany
daniel.buschek@ifi.lmu.de

Florian Alt
Bundeswehr University Munich, Germany
florian.alt@unibw.de

This paper appeared at the Mobile HCI ’18 workshop *Mobile Privacy and Security for an Aging Population*.
https://csalsa.gitlab.io/mobilehciageing/

Abstract
Older adults often rely on the support of trusted individuals (e.g., younger family members) when performing complex tasks on their mobile devices, such as configuring privacy settings. However, a prominent problem is that systems are designed with the intention of a single “main user” using them, with little to no support for cases where the user would like to get external help from others. In this work, we provide anecdotal evidence of problems faced by supporters who try to help older adults in privacy and security related tasks. We outline multiple suggestions for future work in this area, and discuss how systems can support people who support older adults.

Author Keywords
Older adults; privacy; security; mobile devices

ACM Classification Keywords
H.5.m [Information interfaces and presentation (e.g., HCI)]: Miscellaneous; K.6.4 [Security and Protection]

Introduction and Motivation
Older adults increasingly adopt smartphones and tablets. This can be attributed to the fact that many of today’s older adults were younger when mobile devices became ubiquitous, and due to many older adults accepting the adoption of technology [6, 7]. However, this user group may face

specific problems when using their smartphones. For example, older adults might be accustomed to receiving a manual for technological products. Yet, with fast update rates and access to hundreds of thousands of apps [1], today's manuals would often be outdated by the time they are printed. To overcome issues like this, many older adults rely on trusted individuals, such as family members or friends, to help them with tasks on their mobile devices [2, 3, 4, 5]. This includes tasks related to security and privacy, such as configuring privacy settings of mobile apps.

In general, we see two ways of addressing this situation: First, customized solutions could be designed to support older adults in making good security and privacy decisions. Second, such solutions could be designed to facilitate help from trusted individuals, that is, to support people in supporting older adults. Here, we focus on the second approach, which might be more suitable for people who are not confident that they can perform the tasks themselves, or fear that they might misconfigure or "break" something.

In this work, we call aforementioned trusted individuals *supporters*, highlighting their role in helping others. However, currently supporters themselves face tedious problems: For example, smartphones are fundamentally designed to be used only by their respective owners, and not by third party individuals. This hinders supporters in helping others.

We see many opportunities to support people who support older adults. For example, a system could offer a "supporter role" setting to enable creating accounts remotely for others. Moreover, systems could provide older adults with recommendations based on their supporter's security configurations. This could potentially improve the experience of all parties involved.

In the following, we describe anecdotal evidence and discuss multiple problems that supporters encounter when helping older adults, leading to suggestions for future research in this area.

Stories

We informally report on observations and experiences with privacy and security issues that older adults might have.

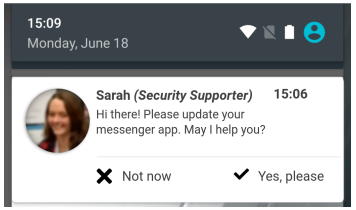
Password Management

We observed older adults managing their passwords in an analogue folder. However, being aware of security issues, they applied a sophisticated way of matching passwords to respective accounts, using ordered numbers and different sheets of paper.

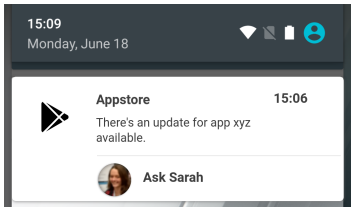
In another example, all three children and even children-in-law were aware of an older adult's password, which was used across multiple accounts. The reason is that the older adult often required help from her family in changing account settings, backing up photos on her smartphone, and so on.

Fallback Authentication

In many cases, supporters are remote and not co-located with the grandparent or parent they are trying to help. In case of phone loss, or setting up a new account on a new phone, situations occur where the older adult needs to remember their account password and email. After failed attempts, the supporter tries to recover the password and email of the older adult using a phone number code. It is often the case that, if the supporter and adult are in two separate countries, the supporter has no access to a local number for code recovery. Such failures of specific fallback authentication cases need to be redesigned.



(a) push



(b) pull

Figure 1: Support for updating an app can either be (a) provided by the supporter (*push*) or (b) requested by the older adult (*pull*).

Figure 2: The supported older adult can access the supporter's advice directly from the security settings screen. Recommendations for security settings can either be given *explicitly* by the supporter or *implicitly* derived from the supporter's own settings.

Privacy Settings
Possible and adequate privacy settings often may be unknown to (elderly) novice users. On the one hand, this is critical when it comes to not applying privacy settings at all. On the other hand, this leads people to finding their own way of protecting their privacy – which might add an unnecessary level of complexity. As an example, we observed older adults using their Android phone without a Google account, which makes many tasks more difficult. At the same time, they installed messenger apps to communicate with their family. As a result, they ran into problems with having to update those apps manually.

Supporting People to Support Older Adults

Based on our observations and anecdotes, we suggest three directions for future investigations into designs for supporting supporters.

Facilitating Communication for Remote Support
Older adults and potential supporters often live apart from each other. This limits the capabilities for direct help. It also makes help requests more tedious to handle, as there are only limited capabilities to provide context (e.g., describe the problem via phone). This could be addressed by giving both sides a medium for communication. Such a solution could include two directions:

- *push:* The supporter is provided with a channel to push relevant information to an older adult. For example, a son could send instructions to upgrade an app, after a security breach for the current version of that app was published (see Fig. 1 (a)).
- *pull:* The other way round, an older adult should get the opportunity to actively request help for a current problem (see Fig. 1 (b)), giving their supporter the necessary context to be able to solve the task.

  One way to address this might be an option to take screenshots and annotate them with concrete questions, allowing the supporter to edit those annotations and provide advice towards the necessary steps.

Integrating Supporter Roles
An idea to "outsource" security is to let older adults choose trusted people to support them in concrete roles. As an example, parents could choose their children as responsible supporters. For instance, supporters could then get the option to actively create accounts for others in a management role: Administrative and security-related tasks (also) remain in the hands of the supporter while the supported user can use the respective service, knowing that security management is in trusted hands.

Supporting Personal Recommendations & Customization
Another idea is to nudge the supported user with suggestions based on the behavior of trusted individuals. For example, a mother accesses a privacy settings screen and receives a prompt asking her if she would like to configure according to her daughter's own setup (compare Fig. 2). Such recommended settings could be created in two different ways:

- *implicit*: Supporters share their own behaviour data with the system, which then shows corresponding recommendations to the supported user (e.g. *"Your daughter uses these settings on her device."*).
- *explicit*: Supporters can explicitly (pre-)configure recommended settings on their own devices for the supported user. These are then suggested to the supported user (e.g. *"Your daughter recommends these settings for you."*).

Conclusion

In this work, we presented anecdotal evidence of problems that occur when older adults seek support from trusted individuals for performing security- and privacy- related tasks. We discussed several directions for future work to address these problems. In future work, we plan to investigate the suggested solutions in detail, as well as conduct empirical studies to better understand and identify even more challenges of supporters of older adults in the context of security and privacy.

Acknowledgements

Work on this project was partially funded by the Bavarian State Ministry of Education, Science and the Arts in the framework of the Centre Digitisation.Bavaria (ZD.B). This research was supported by the Deutsche Forschungsgemeinschaft (DFG), Grant No. AL 1899/2-1.

REFERENCES

1. AppBrain. 2016. Number of available applications in the Google Play Store from December 2009 to February 2016. (February 2016). Retrieved July 29, 2016 from http://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/.

2. Rachel L. Franz, Cosmin Munteanu, Barbara Barbosa Neves, and Ronald Baecker. 2015. Time to Retire Old Methodologies? Reflecting on Conducting Usability Evaluations with Older Adults. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct (MobileHCI '15)*. ACM, New York, NY, USA, 912–915. DOI:http://dx.doi.org/10.1145/2786567.2794303

3. Young Seok Lee. 2007. *Older Adults' User Experiences with Mobile Phones: Identification of User Clusters and User Requirements*. Ph.D. Dissertation. Virginia Polytechnic Institute and State University.

4. Yogesh Malhotra and Dennis F. Galletta. 1999. Extending the Technology Acceptance Model to Account for Social Influence: Theoretical Bases and Empirical Validation. In *Proceedings of the Thirty-Second Annual Hawaii International Conference on System Sciences-Volume 1 - Volume 1 (HICSS '99)*. IEEE Computer Society, Washington, DC, USA, 1006–. http://dl.acm.org/citation.cfm?id=874068.875913

5. Barbara Barbosa Neves, Rachel L. Franz, Cosmin Munteanu, Ronald Baecker, and Mags Ngo. 2015. "My Hand Doesn'T Listen to Me!": Adoption and Evaluation of a Communication Technology for the 'Oldest Old'. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 1593–1602. DOI: http://dx.doi.org/10.1145/2702123.2702430

6. Karen Renaud and Judy van Biljon. 2008. Predicting Technology Acceptance and Adoption by the Elderly: A Qualitative Study. In *Proceedings of the 2008 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries: Riding the Wave of Technology (SAICSIT '08)*. ACM, New York, NY, USA, 210–219. DOI: http://dx.doi.org/10.1145/1456659.1456684

7. Wiktoria Wilkowska and Martina Ziefle. 2009. *Which Factors Form Older Adults' Acceptance of Mobile Information and Communication Technologies?* Springer Berlin Heidelberg, Berlin, Heidelberg, 81–101. DOI: http://dx.doi.org/10.1007/978-3-642-10308-7_6

Digital Mental Health for Older Adults: Privacy Considerations from an Implementation Perspective

Jake Pywell
Northumbria University, Newcastle
jake.pywell@northumbria.ac.uk

Santosh Vijaykumar
Northumbria University, Newcastle
santosh.vijaykumar@northumbria.ac.uk

Abstract
Older adults with depression face a number of barriers to accessing treatment. However, the introduction of computerised Cognitive Behavioural Therapy is a promising salutation to a number of obstacles that older adults encounter. Despite this, older adults are underrepresented in the current literature. Older adults do not engage with technology in the same way as other demographics and have privacy concerns about sharing mental health information which may deter older adults from engaging with interventions and hinder implementation. This paper draws on privacy literature to highlight the need for a greater focus on privacy considerations that older adults may face when engaging with online treatment in order to achieve successful dissemination amongst older adults and to inform policy and design of online mental health interventions.

Author Keywords
Privacy; Depression; Older adults; cCBT; Policy; Implementation.

ACM Classification Keywords
Security and privacy~Social aspects of security and privacy • Security and privacy~Usability in security and privacy

Introduction

Depression is the most prevalent and debilitating mental health condition among older adults, affecting roughly 22% of women and 28% of men in the United Kingdom (UK). Yet, 85% of older adults in the UK fail to receive assistance from the National Health Service (NHS) for depression related symptoms [17]. This problem of access has prompted the emergence of an array of therapies – such as Computerized Cognitive Behavioural Therapy (cCBT) delivered through ubiquitous digital technologies like mobile applications. Issues of user identity information, stigma and confidentiality of data associated with mental health conditions, mean that the widespread institutionalization and adoption of these innovations will be influenced by an understanding of privacy considerations.

The purpose of this paper is to synthesize evidence from related literatures in online mental health interventions and online health information seeking by older adults to demonstrate the urgent need for research that sheds light on the question of interest: What are the privacy concerns of older adults utilizing cCBT services and how can these considerations be incorporated into the design, evaluation and scaling-up of cCBT interventions?

The Problem of Depression

Clinical and subthreshold depression are the biggest cost to mental health services in the UK. However, due to limited number of trained psychotherapists, a lack of help seeking behaviours, stigma and long waiting times, depression is not always treated [9,22]. For example, in England, one in ten people wait more than a year for a mental health assessment [1] with 85% of older people receiving no assistance from the NHS for mental health conditions. These trends are significant given that depression is associated with reduced quality of life, increased disability and increased risk of suicide in the elderly [25]. Even relatively minor levels of depression can lead to a significant decrease in quality of life and negative attitudes towards ageing [3]. It is clearly of great importance to increase older adult's access to mental health treatment.

Online Mental Health Interventions (OMHI) for Older Adults

Older adults face numerous barriers to accessing therapy for depression such as stigma, mobility, and limited number of trained therapists [26]. Over the last decade OMHI have received a great deal of attention due to their potential to tackle barriers to traditional face to face therapy. Literature in this field repeatedly lists accessibility and reach of online mental health interventions to be one of the main advantages [19,23], which seems particularly pertinent to older adults who may be suffering with pain, poor mobility or other chronic illnesses which are barriers to them receiving face to face therapy.

Computerised Cognitive Behavioural Therapy (cCBT) is one type of OMHI and is based on the CBT principles utilised in common treatment for mild and moderate depression. cCBT can be delivered through mobile applications (apps) and online internet sites. Currently the National Health Service (NHS) in England have attempted to introduce a small number of cCBT apps into their stepped care model. There are currently five apps available that utilise CBT principles however there are only two that specifically address mild to moderate depression.

Much of the research supporting the evidence base for cCBT to allow its integration within the NHS has been conducted predominately on adults between 18 and 50

years of age and therefore older adults are dramatically underrepresented in cCBT research. In the limited number of studies conducted for older adults and OMHI, the results have been somewhat positive, suggesting that older adults may respond well to cCBT. For example, a number of Randomised Control Trials (RCT) specifically targeting the older adult demographic have found positive effects for symptom reduction (and at 3 and 12 months follow up), acceptability, satisfaction and adherence, measured by completion rate [6,7,24].

However, outside of a research environment, older adults do not respond to technologies in the same way as other age demographics. Older adults tend to adopt new technologies much later, which may predict greater reluctance to engage with cCBT [5]. Furthermore, older adults are much more cautious about disclosing information while online, particularly in the context of physical and mental health, as they seek to maintain a positive self-image and avoid negative stigma [16]. This presents challenges that need to be overcome for the successful implementation of online interventions for use by older adults.

Privacy for OMHI among Older Adults

Privacy is a factor that features very little in the literature for online CBT. Given the paucity of literature and policy surrounding privacy in OMHI there is a need to draw upon evidence from other domains to inform design and implementation decisions. Previous privacy literature suggests when using online interventions older adults undergo a cost-benefit trade off whereby they may disclose information in order to receive the benefits of reduced symptom severity and not being subject to stigma [15]. Therefore, older adults must perceive cCBT to be more beneficial to them than not receiving therapy/going in person, in order to share their mental health information.

One way cCBT may achieve this is by allowing older adults to access therapy in their own home where they are free from stigmatisation, which has been identified as a key barrier for older adults accessing therapy [4]. This creates a relationship between physical privacy and online privacy worth examining. On the one hand, users may physically isolate themselves in order to engage with the online material, but by doing so are having to share personal, and often sensitive, information about themselves through the digital online application. Physical solitude and isolation have been well documented in privacy literature as types and functions of privacy [20,28,29], so it is perhaps unsurprising that online mental health interventions can help users avoid the stigma of face to face therapy. This trade-off between physical privacy and online privacy may in fact act as a facilitator for older adults wishing to engage in therapy without being subject of stigmatisation.

On the other hand, a recent paper has found that older adults are very cautious when it comes to sharing health information using technology – particularly information specifically relating to mental health as they classify mental health information as sensitive [16]. This may present a barrier for older adults when participating with online mental health technologies in the UK as some of the NHS endorsed apps encourage sharing of mental health information. For example, the 'Catch it' app, encourages users to rate their mood, reflect on thoughts and feelings and collects data about mood and location. Similarly, 'Big White Wall', uses online tests to measure anxiety and depression levels to set goals and track progress. Older adults may be cautious about engaging with these specific apps because for older adults, symptoms of depression are perceived to be associated with cognitive impairment and decline. It is also common for older adults to perceive depression is a natural part of ageing (Law, Laidlaw, & Peck, 2010) instead of a mental health condition, which contributes to the misconceptions older adults have about mental health [2]. Therefore, in order for older adults to engage with this technology and participate in the sharing of sensitive

information, it relies on the fact that they trust their information is stored correctly and confidentially [10], and they feel as though they are free from risk of stigmatisation to maintain a positive self-image.

Although there are arguments for privacy to be a facilitator and a barrier for older adults when engaging with OMHI, the arguments are speculative at this point in time as there is a large gap in the literature when addressing privacy concerns for OMHI in general, but more specifically for older adults. While some OMHI have considered privacy concerns by providing anonymity to encourage free and open expression (e.g. Big White Wall), there is no evaluation of how older adults engage with this facility given their cautiousness when sharing health information online. Therefore, this paper calls for future research to study how older adults engage with OMHI to address privacy concerns.

Privacy as a key Implementation Construct

Privacy as an implementation barrier should also be considered by researchers, practitioners and policy makers. In the translation of CBT from face to face to online applications, privacy has not been considered to the same extent. A qualitative study with key stakeholders, policy and information technology informants found that there is insufficient privacy protection around personal health information and there is a lack of knowledge and expertise around cybersecurity in online mental health care [30]. This finding has been supported by interviews with therapists, who raised concerns over data protection and data security [27]. Although the clients did not share this concern in this particular study, it still poses an implementation issue as therapists will be the ones administering and recommending cCBT in primary care, and if they have negative attitudes towards its use then they are unlikely to recommend it to their patients.

Clearly there is a need to ensure that the privacy policies surrounding online mental health are legally fit for purpose, and adhere to the same standard of confidentiality that face to face therapy offers [12]. There is also a need for this to be portrayed to older adults in a way that they can easily understand. Further advances in the field of OMHI will refine privacy policy to ensure users' information is protected. However these developments may present an avoidable barrier to use given the preconceptions older adults have towards mental health, privacy and technology, unless communicated effectively to the older adult demographic using strategies that are accessible and easily understood.

Failure to consider privacy concerns can cripple the scalability of OMHI and its potential to reach older adults who fear stigmatisation. This is evidenced by the fact that privacy concerns have been identified as a reason for discontinuation of an intervention by participants [8]. However qualitative data detailing the participant's specific privacy concerns have not been gathered by researchers so it is difficult to provide meaningful design implications from the studies conducted to date. Qualitative research validates quantitative findings by providing rich insights into participant's thoughts attitudes and feelings which drive behaviour decisions. Therefore, the value of qualitative data in privacy considerations for OMHI cannot be understated as researchers have called for future research to gather qualitative information to explain specifically why participants drop out [12]. Until privacy concerns of both, the therapist and user have been addressed it is difficult to speculate how successful the diffusion and uptake of OMHI's 'in the wild' will be.

One way in which scalability and implementation challenges of OMHI interventions can be improved is to apply an implementation framework. RE-AIM (reach, effectiveness, adoption, implementation, maintenance) is a framework commonly referred to within the field of

implementation science to evaluate dimensions most relevant to real-world implementation [11,13]. Briefly, *reach* refers to the percentage and characteristics of people receiving the treatment; *effectiveness* is the impact of the intervention; *adoption* concerns the percentage and representativeness of services that adopt the intervention; *implementation* refers to the consistency and cost of delivering the intervention and *maintenance* refers to long-term sustainability [13].

For the successful implementation of OMHI for older adults, privacy concerns should be considered at each stage of the implementation process - particularly in the reach, implementation and maintenance dimensions. These are key dimensions in the RE-AIM framework to tackle privacy concerns as the appropriateness of an intervention can be hindered if privacy concerns of older adults are not considered, given that they have a number of different characteristics in the way they approach technology and mental health. Similarly, if an intervention is well maintained and has long term use, users should be informed what will happen to their information if they choose to disengage with the intervention. Utilising the RE-AIM framework may also encourage interdisciplinary collaboration between researchers, designers, policy makers and end users to ensure a holistic approach is taken when designing OMHI with the consideration of privacy.

Research and Policy Recommendations

cCBT represents a major advance in how therapy is delivered and shows promising potential to overcome barriers to treatment that face to face therapy has encountered. In order to ensure the privacy needs of older adults are considered, and to ensure older adults are properly represented in cCBT literature, a participatory approach to design should be encouraged. While qualitative research is starting to emerge describing user experience and attitudes towards online CBT [14,21], these do not specifically account for older adults, or their privacy preferences. Mohr, Weingardt, Reddy, & Schueller [18] have specifically called for a user-centred design approach to be employed from the earliest exploratory design stages to understand the needs, goals, limitations and capabilities of stakeholders. This is particularly pertinent to older adults as they are already underrepresented in the literature to date.

While older adults are cautious about sharing mental health information, research suggests they are more likely to engage and share information if company endorsements are clearly visible as this increases trust [31]. It would therefore be valuable for future research to investigate whether privacy concerns are present even if a mobile mental health app is endorsed by the NHS, or other health service, as this has not yet been investigated within the area of online CBT for older adults.

As this area of research develops, findings may well suggest that older adults do not engage with the types of online interventions that have already been released onto the NHS apps library. This would then raise questions about whether online mental health interventions can take a 'one size fits all' approach or whether designers of OMHI should design specifically for older adults.

Conclusions

This paper has argued that although privacy may represent both a barrier and facilitator for older adults accessing OMHI, there is still a large gap in the literature, with many questions relating to older adult's privacy preferences remaining unanswered. As a result, there is a need for future research to focus on qualitative methods to understand and address privacy considerations older adults may face when engaging with OMHI. To address the gap in research and in order to implement OMHI's into 'the wild' there should be a focus on interdisciplinary and inter-sectoral research

approaches between all key stakeholders to foresee and overcome barriers to successful engagement for older adults.

References

1. M. R. Bennion, G Hardy, R. K. Moore, and A. Millings. 2017. E-therapies in England for stress, anxiety or depression: What is being used in the NHS A survey of mental health services. *BMJ Open* 7, 1.

2. G.A Brenes, S.C Danhauer, M.F Lyles, P.E Hogan, and M.E Miller. 2015. Barriers to Mental Health Treatment in Rural Older Adults. *The American journal of geriatric psychiatry : official journal of the American Association for Geriatric Psychiatry* 23, 11: 1172–8.

3. E Chachamovich, M Fleck, K Laidlaw, and M Power. 2008. Impact of Major Depression and Subsyndromal Symptoms on Quality of Life and Attitudes Toward Aging in an International Sample of Older Adults. *The Gerontologist* 48, 5: 593–602.

4. K.O Conner, V.C Copeland, N.K Grote, et al. 2010. Mental health treatment seeking among older adults with depression: the impact of stigma and race. *The American journal of geriatric psychiatry : official journal of the American Association for Geriatric Psychiatry* 18, 6: 531–43.

5. Rebecca M. Crabb, Kate Cavanagh, Judy Proudfoot, Despina Learmonth, Samantha Rafie, and Kenneth R. Weingardt. 2012. Is computerized cognitive-behavioural therapy a treatment option for depression in late-life? A systematic review. *British Journal of Clinical Psychology* 51, 4: 459–464.

6. Blake F Dear, Judy Zou, Nickolai Titov, et al. 2013. Internet-delivered cognitive behavioural therapy for depression: A feasibility open trial for older adults. *Australian & New Zealand Journal of Psychiatry* 47, 2: 169–176.

7. Blake F. Dear, Judy B. Zou, Shehzad Ali, et al. 2015. Examining self-guided internet-delivered cognitive behavior therapy for older adults with symptoms of anxiety and depression: Two feasibility open trials. *Internet Interventions* 2, 1: 17–23.

8. G Doherty, D Coyle, and J Sharry. 2012. Engagement with Online Mental Health Interventions: An Exploratory Clinical Study of a Treatment for Depression. *Proceedings of SIGCHI conference on Human Factors in Computing Systems*.

9. Filip Drozd, Linda Vaskinn, Hans Bugge Bergsund, Silje Marie Haga, Kari Slinning, and Cato Alexander Bjørkli. 2016. The Implementation of Internet Interventions for Depression: A Scoping Review. *Journal of medical Internet research* 18, 9: e236.

10. Shira H. Fischer, Daniel David, Bradley H. Crotty, Meghan Dierks, and Charles Safran. 2014. Acceptance and use of health information technology by community-dwelling elders. *International Journal of Medical Informatics* 83, 9: 624–635.

11. R.E Glasgow, T.M Vogt, and S.M Boles. 1999. Evaluating the Public Health Impact of Health Promotion Interventions: The RE-AIM Framework. *American Journal of Public Health* 89, 9.

12. C Hill, C Creswell, S Vigerland, MH Nauta, and S March. 2018. Navigating the development and dissemination of internet cognitive behavioral therapy (iCBT) for anxiety disorders in children

and young people: A consensus statement with recommendations from the #iCBTLorentz Workshop Group. *Internet Interventions 12*: 1–10.

13. D.K. King, R.E. Glasgow, and B. Leeman-Castillo. 2010. Reaiming RE-AIM: using the model to plan, implement, and evaluate the effects of environmental change approaches to enhancing population health. *American journal of public health* 100, 11: 2076–84.

14. Sarah E Knowles, Karina Lovell, Peter Bower, et al. 2015. Patient experience of computerised therapy for depression in primary care. *BMJ Open* 5.

15. Linda Little, Ruth Laidler, Pam Briggs, and Lynne Coventry. 2010. Who has access? Understanding sensitivity and disclosure of information. *Symposium On Usable Privacy and Security (SOUPS) 2010*.

16. A McNeill, P Briggs, J Pywell, and L Coventry. 2017. Functional privacy concerns of older adults about pervasive health-monitoring systems. *In Proceedings of PETRA 2017* ACM Press.

17. Mental Health Foundation. 2015. Mental health statistics: older people. Retrieved April 9, 2018 from https://www.mentalhealth.org.uk/statistics/mental-health-statistics-older-people.

18. DC. Mohr, KR. Weingardt, M Reddy, and SM. Schueller. 2017. Three Problems With Current Digital Mental Health Research . . . and Three Things We Can Do About Them. *Psychiatric Services* 68, 5: 427–429.

19. J Newton and E C Sundin. 2018. A questionnaire-based qualitative study of therapist views on computerized CBT. *The Cognitive Behaviour Therapist* 9, 15: 1–14.

20. DM Pedersen. 1997. Psychological functions of privacy. *Journal of Environmental Psychology* 17: 147–158.

21. S. Rennick-Egglestone, S. Knowles, G. Toms, P. Bee, K. Lovell, and P. Bower. 2016. Health Technologies "In the Wild": Experiences of Engagement with Computerised CBT. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (pp. 2124-2135). ACM.*

22. T. Rost, Stein, Margrit Löbner, Anette Kersting, Claudia Luck-Sikorski, and Steffi G Riedel-Heller. 2017. User Acceptance of Computerized Cognitive Behavioral Therapy for Depression: Systematic Review. *Journal of medical Internet research* 19, 9: e309.

23. Johanna Schröder, Thomas Berger, Stefan Westermann, Jan Philipp Klein, and Steffen Moritz. 2016. Internet interventions for depression: new developments. *Dialogues in clinical neuroscience* 18, 2: 203–12.

24. L.G Staples, V.J Fogliati, B.F Dear, O Nielssen, and N Titov. 2016. Internet-delivered treatment for older adults with anxiety and depression: implementation of the Wellbeing Plus Course in routine clinical care and comparison with research trial outcomes. *BJPsych open* 2, 5: 307–313.

25. N Titov, VJ Fogliati, LG Staples, et al. 2016. Treating anxiety and depression in older adults: randomised controlled trial comparing guidedv. self-guided internet-delivered cognitive-behavioural therapy. *BJPsych open* 2, 1: 50–58.

26. Nickolai Titov, Blake F. Dear, Shehzad Ali, et al.

2015. Clinical and Cost-Effectiveness of Therapist-Guided Internet-Delivered Cognitive Behavior Therapy for Older Adults With Symptoms of Depression: A Randomized Controlled Trial. *Behavior Therapy* 46, 2: 193–205.

27. R Waller and S Gilbody. 2009. Barriers to the uptake of computerized cognitive behavioural therapy: a systematic review of the quantitative and qualitative evidence. *Psychological medicine* 39, 5: 705–712.

28. AF Westin. 1967. *Privacy and Freedom*. New York.

29. AF Westin. 2003. Social and political dimensions of privacy. *Journal of social issues*.

30. Lori Wozney, Amanda S. Newton, Nicole D. Gehring, et al. 2017. Implementation of eMental Health care: viewpoints from key informants from organizations and agencies with eHealth mandates. *BMC Medical Informatics and Decision Making* 17, 1: 78.

31. D.M Zulman, M Kirch, K Zheng, and L.C An. 2011. Trust in the internet as a health resource among older adults: analysis of data from a nationally representative survey. *Journal of medical Internet research* 13, 1: e19.

Designing Authentication with Seniors in Mind

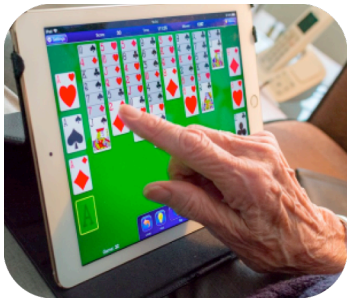


Figure 1: Seniors enjoying their digital devices (Images from Pixabay by Sabine van Erp & Jérôme Choain)

Karen Renaud
Kenneth Scott-Brown
Andrea Szymkowiak

Abertay University
Dundee, UK DD1 1HG, UK
k.renaud@abertay.ac.uk
k.scott-brown@abertay.ac.uk
a.szymkowiak@abertay.ac.uk

Abstract

Developers typically adopt perceived best practice, and in the case of authentication this means password security. However, given the wide range of technical solutions available and the diverse needs and limitations of older users, we suggest that the default adoption of electronic "username and password" authentication may not be 'best practice' or even good practice. This paper highlights some challenges faced by three seniors, each of whom has multiple age-related disabilities and concomitant life challenges. The result is that they cannot authenticate themselves when they need to access their devices and accounts. We conclude by suggesting a number of research directions calculated to address some of these challenges and promote inclusive design and allow for diverse user authentication.

Author Keywords

Authentication; Seniors; Accessibility;

ACM Classification Keywords

• Human-centered computing~Accessibility theory, concepts and paradigms
• Human-centered computing~Accessibility design and evaluation methods.

Introduction

The EU commission states that 80 million people in the EU are affected by a disability. As the EU population ages this number is predicted to increase to 120 million by 2020. There is a need to design for accessibility so that the elderly can participate equally and actively in society [6]. The UN Convention on the Rights of Persons with Disabilities contains accessibility obligations [20] and requires Member States to accommodate those with disabilities. It is almost 10 years since they published this manifesto, but there is not much evidence that it has been taken to heart, especially when designing authentication mechanisms.

We would like to introduce three *fictitious* senior citizens to illustrate the difficulties they are likely to face when interacting with technology and to highlight their needs.

Vera is 81 years old and lives independently, despite a number of health issues. Her metabolism has slowed to such an extent that her fingers are always cold. She is more or less housebound due to severe arthritis. She can hear with her brand new hearing aid, but experiences difficulty remembering things these days.

Vera's proudest possession is her iPad, with her iPhone a close second. She is having some problems though: she has managed to lock herself out of her iPhone and needs to sign into her iCloud account on her iPad to reactivate it. Her fingers are too cold for the fingerprint reader to pick up, and she finds that she has forgotten the PIN. She eventually finds the bit of paper she wrote it on. She now needs to sign into iCloud, with its 14-character password. This is extremely frustrating because she forgets where she is halfway through as she types it in, and finds that holding the Shift key down while she types is hard with her arthritic fingers. Actually, she only needs to tap it, but she is erroneously applying her "typewriter" mental model to the situation. She subsequently also gets locked out of her iCloud account. She has to wait two weeks for her daughter to come and visit her before the situation can be resolved.

John, 75, receives an email from what claims to be his email provider, asking for credentials. The phisher takes over his email account and he cannot figure out how to contact Microsoft. A cleaner arrives, and John has to ask for her assistance to resolve the problem. This takes 2 hours and the cleaner has no time to clean his apartment. She also feels uncomfortable because she now possesses personal details belonging to her client.

Jo is 90 years old, with early stage dementia, depression and delirium. Jo can physically navigate the home but is unable to operate a TV remote or a telephone. Judged fit to be discharged from hospital, Jo is sent home and is still expected to run a current account with a debit card, even though housebound. Jo asks a neighbor to draw money, and he does this, but also helps himself to £100 and claims he delivered all the money. Because of the dementia, no one believes Jo's version of the event and the neighbor gets away with the theft.

These vignettes, loosely based on the authors' personal contacts, demonstrate how the *de facto* authentication mechanisms of the 21st century are failing to meet the needs of our older population. Our seniors have multiple health issues and are often lonely and poorly

supported. The industry's focus on designing mechanisms with the able-bodied in mind, under the assumption that the end user will be familiar with the mechanisms and dangers of the digital world, leaves seniors frustrated, excluded and vulnerable to hacking attacks and fraud.

Authenticating someone at a distance, especially digitally, is nontrivial. The digital world generally makes use of a shared secret to achieve this but, as we shall show, this is suboptimal, especially for our seniors.

Consider the advice usually given to password creators: (1) create a password that is essentially nonsense, that no one can guess, and (2) don't write it down [11]. Even for young people with agile minds this is taxing. Yet this advice is even more difficult to follow if you are aging and your memory is not as sharp as it used to be. Other password advice mandates complexity, which makes passwords hard to input with arthritic fingers, even if they can be remembered.

In this paper, we outline the challenges faced by senior citizens needing to authenticate themselves. We then discuss a number of research opportunities that ought to be considered when designing an accessible authentication mechanism that will not exclude, alienate or render senior users vulnerable to exploitation [1, 14].

Challenges to Seniors

Inaccessible Interfaces

Many of the elderly of today did not use computers during their working lives. This means that they have no mental models to match the interfaces they have to engage with when they used the latest technologies. Moreover, technology changes much faster than they are comfortable with, often leaving them feeling disoriented. It takes them longer to process changes and the speed of change means them feeling as if they are never catching up.

Inaccessible Authentication

The most widely-used authentication mechanism is the password, perhaps because of it was the first mechanism used to control access to computers [13] or because the choice of a password represents the least effort for developers [18]. Yet many people struggle with passwords, and the aged find them particularly troublesome [8]. Design guidelines for senior-sensitive design cannot be used to inform authentication design because they maximize feedback and error correction [12]. Because authentication is security-related, this conflicts with good practice.

Passwords rely on the ability to remember a long nonsense string. This ability severely declines as we age [19]. Passwords arguably fail the accessibility test when the user base includes older users.

Some researchers have designed picture-based passwords in order to make authentication less burdensome in terms of memory [16, 17]. Others have exploited the fact that music memory is more permanent and erodes less easily than memory of character strings [7]. These have not enjoyed widespread uptake.

Some devices are now routinely released with inbuilt fingerprint or face biometric readers. Our first vignette shows that this seemingly effortless mechanism fails for

many users, due to age-, disability- or health-related infirmities [3].

The other alternative is the use of a token, something the user owns. However, dementia and Alzheimers, diseases that strike predominantly older users, will make them lose or misplace these [10]. Moreover, many tokens are used in conjunction with a PIN or password, which is also likely to be forgotten.

Supported Living

Many seniors become increasingly reliant on family members, merely to get through their usual day-to-day lives. The overwhelming majority of such carers would not dream of exploiting their relatives but there are exceptions [5].

However, many do not have a family member or trusted friend to help them. Many do need help authenticating, especially now that governments routinely deposit pensions and benefits into people's bank accounts [4]. The question is how those who need support elicit help without opening themselves up to fraud and theft.

Seniors are familiar with hard cash, not with using a card to pay for goods and services. Society has moved to card payments and online banking, and are often given no choice in the matter [4]. Yet age-related infirmities and mobility issues are a major obstacle. How does an older person draw cash from the bank when they cannot get to the bank themselves? The banks do not offer any mechanisms to support this. When people are unable to access their own money, they are left feeling helpless and disempowered. Even worse, they are forced into violating the terms of use of their account in order to get cash, eliciting assistance from helpers, friends and family. Any subsequent fraud will be blamed on the account holder rather than the fact that a system has not been designed to accommodate their limitations.

Why Authenticate?

Before we talk about solutions, we need to take a close look at exactly what the purpose of authentication is. Essentially, authentication confirms that the person claiming identity has a right to claim it. Kent and Millet say there are two reasons for such confirmation being important: (1) Accountability, and (2) Authorization [11].

In the first case, authentication is carried out so that users can be held accountable for their actions while using the system. In the second case, people are permitted to carry out particular actions based on their confirmed identity: they are *authorized* to do so.

Does either of these justifications apply to Vera using her iPad? Vera is not accountable to anyone else for what she does to her own device. By dint of ownership she has no need to be authorized. It seems that a third reason for authenticating is coming into play here: preventing 3rd party usage. If someone were to steal the iPad, they would not, theoretically, be able to use it because authentication is required.

In other words, Vera is being required to authenticate multiple times a day just in case someone steals her iPad. The cumulative cost to Vera, and the frustration that results if she is locked out after three tries, is not factored into the design of the mechanism. A more usable solution would allow more attempts, or allow

authentication by proxy where a trusted family member could help her remotely if she forgets her password.

If accessibility were taken seriously, the government would not force Jo to engage with a digital world when she is cognitively and physically unable to do so. Those who provide pensions are, by definition, dealing with some of the most vulnerable members of society. More flexibility and indeed, genuine accessibility, would not go amiss.

The UN's Article 9 mandates the following with respect to assuring accessibility for the disabled[1] (we only report those items relevant to authentication). The identification and elimination of obstacles i.e. to:

(1) provide information, communications and other services, ***including electronic services*** and emergency services,

(2) monitor the implementation of minimum standards and guidelines for the ***accessibility of facilities and services open or provided to the public,***

(3) provide training for stakeholders on ***accessibility issues*** facing persons with disabilities,

(4) ***promote other appropriate forms of assistance*** and support to persons with disabilities to ensure their access to information,

(5) promote access for persons with disabilities to new information and communications technologies and systems, ***including the Internet,*** and

(6) promote the design, development, production and distribution of accessible information and communications technologies and systems at an early stage, ***so that these technologies and systems become accessible at minimum cost.***

There is little evidence, when one listens to the experiences and anecdotes reported by the elderly, that these guidelines are being taken note of and adhered to.

Opportunities

We now describe some design recommendations for further research when implementing accessible authentication technology for the elderly.

Authentication – Accessible Implementation

Password requirements that mandate complexity (upper case, lower case, digits and special characters) are particularly problematical. This is so especially when they encourage the invocation of the incorrect mental models, such as the example of Vera holding down the shift key, instead of tapping it. Mandating inclusion of special characters requires seniors to switch soft keyboards, something they have no mental model for. Moreover, many systems obfuscate password entry. Age-related short-term memory decline [15] leads to people forgetting where they are in terms of entering the password. This leads to multiple entry attempts, and possibly getting locked out.

---

1 https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities/article-9-accessibility.html

Authentication – At Home, But Not Alone

When people authenticate on their own devices they are not being authenticated to hold them accountable, or to authorize them. It is being carried out to protect their devices in the case of theft. Bonneau *et al*. [2] argue for technological "smarts" to be used to augment passwords in order to achieve a more reliable authentication.

For example, a more innovative way to authenticate Vera would permit device usage from one particular network or location without deliberate authentication being required. Proof of identity, by engaging in authentication, could only be required if the device is used from a different location.

When authentication is unavoidable, such as when money is being drawn from a bank account, or a purchase is being made from their device, innovation could deliver more accessible solutions.

For example, the older person could nominate a trusted person to carry out a proxy sign-in on their behalf: assisted sign in. Social support has been shown to be a powerful motivator in terms of modern technology usage [9]. Clearly the older person and the trusted "other" would pre-arrange a protocol in advance. This might be a phone call, or the older person being identified by a person at the bank branch, and then contacting the trusted other.

People are told never to share their PINs, but the issue of housebound people being unable to draw cash is not considered. Banks ought to offer a mechanism for one-time expiring PINs to be issued, linked to a particular withdrawal amount. This would allow the person to ask someone else to withdraw cash for them, without being worried about the person emptying their account, or reusing the PIN multiple times.

If the senior uses their own iCloud (or equivalent cloud storage service) account from their home location, an assisted login would also free them from the burden of password retention.

Conclusion

In this paper, we have sought to highlight the challenges facing the elderly who have multiple age-related disabilities. We discuss opportunities for research to address the identified issues. Although the UN Human Rights charter mandates accessibility, there is little evidence that this human right is being enjoyed by the elderly. It is important for designers to start thinking about this market, especially because it is growing at an unprecedented rate and will incorporate future seniors, including ourselves.

References

1. Anon. 2018. FRAUD ALERT: Elderly Harrogate woman conned out of £9,200 in courier fraud. https://northyorkshire.police.uk/news/courier-fraud-alert-elderly-harrogate-woman-conned-9200/ (Accessed 20 April 2018)
2. Bonneau, J., Herley, C., Van Oorschot, P.C. and Stajano, F., 2015. Passwords and the evolution of imperfect authentication. Communications of the ACM, 58(7), pp.78-87.
3. bromba.com. Bioidentification: Frequently Asked Questions. Accessed 26 April 2018 http://www.bromba.com/faq/biofaqe.htm
4. Citizens Advice Bureau. undated. Payment of benefits and tax credits. https://www.citizensadvice.org.uk/benefits/benefits

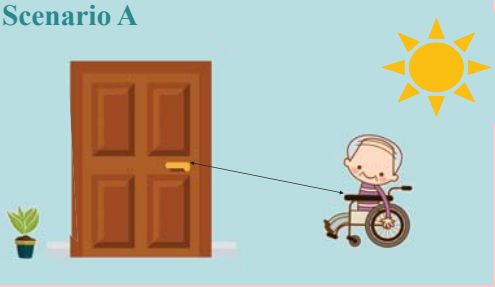
-introduction/payment-of-benefits-and-tax-credits/ (Accessed 20 April 2018)

5. Doherty, S. 2018. Obsessive boyfriends, child abusers and the woman who defrauded her mother - Kent criminals who abused positions of power and trust. 12 April. https://www.kentlive.news/news/kent-news/kent-criminals-who-despicably-abused-1450430 (Accessed 20 April 2018)
6. EU. Commission proposes to make products and services more accessible to the disabled persons. http://europa.eu/rapid/press-release_IP-15-6147_en.htm (Accessed 20 April 2018)
7. Gibson, M., Renaud, K., Conrad, M. and Maple, C., 2009, September. Musipass: authenticating me softly with my song. In Proceedings of the 2009 workshop on New Security Paradigms Workshop (pp. 85-100). ACM.
8. Helkala, K., 2012, August. Disabilities and authentication methods: Usability and security. In Availability, Reliability and Security (ARES), 2012 Seventh International Conference on (pp. 327-334). IEEE.
9. Hill, R., Beynon-Davies, P. and Williams, M.D., 2008. Older people and internet engagement: Acknowledging social moderators of internet adoption, access and use. Information Technology & People, 21(3), pp.244-266.
10. Ishii, H., Kimino, K., Aljehani, M., Ohe, N. and Inoue, M., 2016. An Early Detection System for Dementia Using the M2 M/IoT Platform. Procedia Computer Science, 96, pp.1332-1340.
11. Kent, S. and Millet, L. 2003. Who Goes There. Authentication Through the Lens of Privacy. The National Academies Press. Washington.
12. Kurniawan, S. and Zaphiris, P., 2005, October. Research-derived web design guidelines for older people. In Proceedings of the 7th international ACM SIGACCESS Conference on Computers and Accessibility (pp. 129-135). ACM.
13. Morris, R. and Thompson, K., 1979. Password security: A case history. Communications of the ACM, 22(11), pp.594-597.
14. Mulligan, S. 'Despicable' fraudsters who targeted elderly victims sentenced. http://www.sthelensstar.co.uk/news/16167215._Despicable__fraudsters_who_targeted_elderly_victims_sentenced/ (Accessed 20 April 2018)
15. Murphy, D.R., Craik, F.I., Li, K.Z. and Schneider, B.A., 2000. Comparing the effects of aging and background noise on short-term memory performance. Psychology and Aging, 15(2), p.323.
16. Renaud, K., 2006. A visuo-biometric authentication mechanism for older users. In People and Computers XIX—The Bigger Picture (pp. 167-182). Springer, London.
17. Renaud, K. and Ramsay, J., 2007. Now what was that password again? A more flexible way of identifying and authenticating our seniors. Behaviour & Information Technology, 26(4), pp.309-322.
18. Renaud, K. and Maguire, J., 2013, May. Shrinking the Authentication Footprint. In EISMC (pp. 2-11).
19. Salthouse, T.A., 2003. Memory aging from 18 to 80. Alzheimer Disease & Associated Disorders, 17(3), pp.162-167.
20. UN. 2009. Convention on the Rights of Persons with Disabilities (CRPD) https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html (Accessed 20 April 2018)

Mobile Access Control System through Biometric Recognition for Elderly

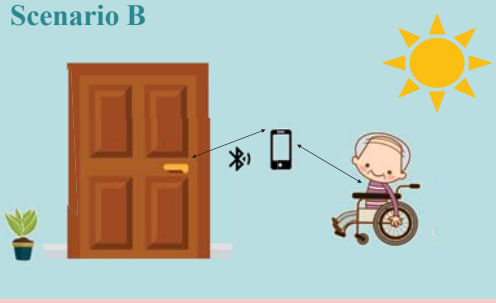
Barbara Corsetti[1], Ramon Blanco-Gonzalo[1], Elakkiya Ellavarason[2], Raul Sanchez-Reillo[1]
[1]University Group for Identification Technologies (GUTI)
Univerisity Carlos III of Madrid, Leganes (Spain)
[2]School of Engineering and Digital Arts
University of Kent, Canterbury (UK)
[1]{bcorsett, rbgonzal, rsreillo}@ing.uc3m.es / [2]e.ellavarason@kent.ac.uk

Scenario A



Fingerprint sensor embedded on the door lock

Scenario B



Fingerprint recognition on a smartphone

Scenario C

Face recognition trough a camera located above the door

Scenario D

Face recognition on a smartphone

Elderly people face lots of accessibility barriers every day.

We propose a biometric recognition-based system that helps people to perform one of the most common daily task: **opening a door**. The system has been developed particularly for elderly people with **accessibility concerns**.

Four scenarios are investigated in order to evaluate the user interaction in different approaches.

An **App** helps users completing tasks in two scenarios (B and D).

The evaluation has been carried out following the **ISO/IEC 21472**.

Biometrics may achieve high level of **security** in control systems, avoiding physical barriers and easing daily tasks.

ACM 2018 – Barcelona

Curious? Send an email to the Author:

This work has been supported by Marie Skłodowska-Curie EU Framework for Research and Innovation Horizon 2020, under the Grant Agreement No. 675087 within AMBER (enhanced Mobile BiomEtRics).