"I simply accept the terms and conditions so that I can use an app at all": Smartphone Use and Privacy among Older Adults in Switzerland

Speck Sarah[1][0000-0002-9076-4121], Cora Pauli[1][0000-0001-7925-6073], Cornelia Ursprung[1][0000-0001-7796-2759], Miriam Wallimann[1] [0000-0002-0238-7187] Robert Huber[2], Sabina Misoch[1][0000-0003-0791-4991]

[1] Institute for Ageing Research, University of Applied Sciences of Eastern Switzerland, Rosenbergstrasse 59, 9001 St.Gallen, Switzerland
[2] Pappy GmbH, Flüelastrasse 6, 8048 Zurich, Switzerland
sarah.speck@ost.ch

Abstract. Digitalization and ageing population are two of the main trends of the 21st century. Most people, including older adults, are now digitally connected to the world for e.g., managing health and finances and this has become indispensable parts of our lives. A device like a smartphone is easily at hand and ready to use anytime, anywhere. However, this widespread usage produces huge amounts of data, which is not without risks, especially for older users in terms of data protection and privacy. This paper investigates behaviours, attitudes, and experiences regarding privacy settings and take a closer look at the phenomenon of resignation and the privacy paradox within the research project *Easierphone. Easierphone* app *Easierphone* aims to simplify smartphone use for older adults and other vulnerable people by replacing the Android surface with an easier one. For data collection, 30 qualitative interviews and diaries were used during installation and testing of the app. Regarding privacy and data protection, most of our participants stated that they generally do not read the terms of use in the digital world carefully. Nonetheless, they still agree to them, so they can use an app or a digital service which clearly illustrates the privacy paradox.

Keywords: Ageing, Digitalization, Older Adults, Smartphone Use, Privacy, Data Protection, Privacy Paradox, Resignation.

1 Introduction

Digitalization and ageing population are two of the main trends of the 21st century. Most people, including older adults (≥ 60 years), are now digitally connected to the world; online services, i.e., to maintain social connections or for managing health and finances, have become indispensable parts of our lives. A device like a smartphone is easily at hand and ready to use anytime, anywhere. Smartphone ownership per person increased globally to over 83% in emerging economies and over 94% in advanced economies [1]. Older adults in Switzerland also show high use of information communication technology [2], and almost 70% are using smartphones in their daily life [3].

However, this widespread usage produces huge amounts of data, which is not without risks, especially for older users in terms of data protection and privacy as they are less experienced [4, 5]. The increase in smartphone ownership, hence use, are not without consequences as every move and action online generates data and leaving data traces [4]. Leaving data traces happens both, conscious and unconscious. Related to older adults this sometimes also means that they pull back from using digital technologies which van Dijk [6] describes as one of the barriers which restrict access to digital technologies. This is because older adults are more cautious and lack knowledge how to protect their online data. However, over and over the experience is made that for instance information overload, such as terms and conditions for a download of an app, leads to paradoxical behaviour which stands in contrast to their attitude concerning privacy and data protection as users just accept settings [7, 8]. Zeissig et al. [4] found in their studies that the older adults tend to protect their online data and maintain online privacy more than younger generations. Despite this result, they also found that attitude towards online privacy differs from actual behaviour and privacy concerns. The issues of older adults' online privacy behaviours, data protection, and their use of digital devices still need further research (e.g., 4, 9–12). Further, older adults are a special group when it comes to usage of digital technologies, they are more cautious and careful in using these technologies and less experienced than their younger counterparts whom we know as digital natives.

This paper gets in at exactly this point: older adults and their attitudes, behaviours made in the field of privacy and data protection using their smartphones. We investigate their views and experiences they made in general with privacy relating to smartphone use and online activities and their experiences during *Easierphone* testing. *Easierphone* is an app developed in collaboration with Pappy GmbH in the context of the AAL-program funded research project. The app *Easierphone* aims to simplify smartphone use for older adults and other vulnerable people. The app is designed for the less tech-savvy in this heterogenous age group and intends to replace the common Android interface with a simplified, more user-friendly one [13]. Furthermore, *Easierphone* app enables remote access for a trusted assistant (e.g., family members, friends) by mirroring the screen on the assistant's device, so they can give virtual assistance when users face usability problems. Additional functionalities, such as a machine learning algorithm to detect changes in usage behaviours (by measuring screen time) or a step counter, are optional functions within the app. Here the potential end user and our participants are confronted with several questions around privacy and data protection concerning certain *Easierphone* features. Who is allowed to see my steps per day? Who will I give permission to remotely adjust settings on my smartphone? Who do I choose as trusted assistant for the remote assistance?

Within the bigger scope of the project, we here explicitly focus on aspects of privacy for this paper – an important current challenge [11]. Particularly we want to investigate this from a viewpoint of older users. We examine their behaviours, attitudes, experiences, and decisions regarding privacy settings and take a closer look at the phenomenon the privacy paradox [14, 8]. The privacy paradox amongst others describes the fact that older adults are more concerned about online privacy risks but at the same time have fewer protective strategies compared to younger generations [4, 5]. In addition,

we want to carve out the differences between subjective users' perceptions and smartphone providers' objective framework regarding (online) privacy and data protection. With the focus on simplifying older adults' smartphone use, our research project around the *Easierphone* app needs to adhere to Android system requirements for the installation, while still trying to make this process as simple as possible. Users are still required to give several permissions from download to setup of the app, e.g., allowing automatic import of contacts into *Easierphone*'s contact function, or allowing remote access which is required for the assistant functionality. This raises additional questions of privacy and data protection: What data can be accessed by the assistant, e.g., tracking of routes walked, step counter and screen usage data. If enabled, these can be remotely observed by the assistant in their *Easierphone* app. It is a balancing act between the privacy of *Easierphone*'s main user and what data their assistants, or third parties are able or allowed to see, and track. While older adults as main users of the app may think they are being watched and patronized, assistants might have the best intentions. The boundary between useful remote access and someone's privacy being violated can vary strongly between different users' subjective point of view and need to be further investigated to enable improvement for further development [13].

2 Privacy among Older Adults in the Digital World

2.1 Privacy attitudes and behaviors

Privacy research is a large field, rooted in diverse disciplines. "Privacy can and does mean different things to different people" [15] (p. 642 9). In general, there is still lack of an agreed upon definition since privacy appears in many fields of life. However, key of privacy research and definition determination were made by Altman [16] and Westin [17]. Whereas Altman's definition includes limiting social interaction and focuses more on physical space of privacy and territoriality, Westin's definition focuses more on how information about or from persons are dealt with [7].

Hitherto, scholars working on privacy within the context of the digital world and digital technologies mainly align with the information and location sharing preferences [18, 19, 7]. Privacy perceptions and behaviours related to digital technologies have been widely studied in the last decade (see e.g., 20–22) also the question of privacy in the public referring to developments in information and digital technology has been in-depth researched [23].

However, the topic has been less researched with reference to the social group of older adults increasingly using digital technologies, for surfing the web, health services, services for financial issues, and smartphone use for example in daily life. Elueze and Quan-Haase [12] explored attitudes and concerns of older adults' in their digital lives. Based on Westin's typology of privacy types they carved out a total of five privacy types among older adults and found that attitudes and behaviours among older adults are highly diverse ranging from fundamentalists (being suspicious about everything) to marginally concerned ones (see also Courtney [24]). In general, using digital technologies, increases concerns regarding privacy [25]. Among older adults where studies found that most of them are less experienced in the digital world which in return plays

out on low digital literacy. Hence, older adults feel less secure to use digital technology and assess risks with disclosing personal information higher than their younger counterparts. van Dijk's [6] research showed that questions about privacy and security even are main reasons for drawbacks and not using digital technology and among older people as the main barrier for not using digital technologies. Also, Kwasny et al. [26] noted that older adults tend to protect their personal data more than their younger counterparts and that privacy attitude, behaviour and concerns differ among young and old. Interestingly, they found, emerging from data of their studies, that Westin's definition on privacy accords more to younger people, and Altman's definition suits more for older adults in the context of digital technologies.

Generally, older adults have also less experience or understanding of online privacy, strategies of protecting personal data than people who grew up in the digital age. For the present research paper and study, we refer on the concept of privacy paradox and by examining attitudes, behaviours and experiences concerning online privacy in this light we will carve out the most striking topics older persons mention.

2.2 The Privacy Paradox

Talking about privacy, the concerns and behaviour referring to the protection of personal data, privacy paradox is not far off. People trade personal information for benefits; however, their attitude, concern and behaviour vary highly when it comes to disclosure of personal information. For instance, Sayre and Horne [27] found that people freely share information for free benefits (here groceries) in return. Also, certain areas of life are more private than others [28]. Several research on attitude and behaviour related to privacy showed that often attitudes of persons to disclose their personal information (= intention to disclose) are more cautiously made than actual behaviour in this context. Actual disclosure differs significantly from a person's intention or attitude [8, 27]. Norberg et al. [8] for example found in their study about personal information disclosure that intentions of people differ a lot from their actual behaviours, although they seem to be concerned about their personal information and privacy which is known as the privacy paradox. The privacy paradox describes the fact that people are more concerned about their personal information, e.g. in online privacy risks but in parallel have few protective strategies to withhold personal information, or rather are actually more open to share their personal information and disclose when it comes to usage of certain services or benefits (cf. e.g., [5, 4, 29].

Privacy is closely connected to trust and risk. Studies have found that in general a higher risk which is connected to negative outcomes influences the individual's concerns relating to privacy (see e.g., [30]). Trust on the other hand also plays a significant role when it comes to disclosure of personal information. In general, the more known or established a company or institution is, the higher the trust or willingness to disclose information [31]. Notwithstanding, trust depends on the context as it works differently in online or offline contexts [8]. In addition, in the context of privacy, the privacy calculus is a model that explains the paradoxical behaviour: Users weigh up the expected benefits of online transactions against feared privacy risks. If the expected benefits

outweigh the risks, users disclose content despite their fears [32, 33].If the expected benefits outweigh the risks, users disclose content despite their fears [32].

For the present study, we are interested how the privacy paradox appears in attitude and actual behaviour of our older participants in the context of the Easierphone field tests and what older adults' opinions are regarding use of the *Easierphone* app and their smartphones, and further their concerns regarding online privacy in general. Some test persons explicitly mentioned they have no concerns regarding online privacy. For this publication focus on the ones that were expressing concerns.

3 Research Design and Applied Methods

3.1 Easierphone: A Multi-National Project

Easierphone is a multinational European research project funded under the EU Active Assisted Living Programme. The aim of this programme is to promote cooperation between end-users, industry, and research. The project consists of six project partners from Switzerland, the Netherlands, and Poland and has a duration of 30 months (April 2021-September 2023).

The focus of the project is not only to develop an app for older people, but to follow this path in a participatory manner and with participative methods together with the target age group. During the entire project duration, the app is being tested in three successive project phases (pilot 1, 2 and 3) in a real live setting with potential end users (seniors, relatives, caregivers) and continuously developed further based on their feedback. Each participating country is responsible for the national data collection but works with the same survey tools. In pp2, questions of privacy and data protection from the user's point of view are very much in the foreground: On the one hand, specifically related to the use of *Easierphone*, but we also wanted to deepen the perspective of older users on the topic of online privacy in general. During the tests, we meticulously explain to the participants what the app tracks, how tracking can be disabled and how the participants themselves have control over various functions. Also, with respect to the remote access of their assistants.

In each pilot, the IAF team conducts interviews with three single testers and seven tandems (main user plus assistant), resulting in a total of 30 tests in Switzerland. Both, the single testers, and the main users of the tandem must be at least 65 years old. Another inclusion criterion is that the main users own a smartphone but do not feel confident in using it. The living situations of the participating seniors were very diverse, with married, single, and widowed persons participating, some with kids some without. It was important to recruit a diverse sample because the population group "older adults" is very heterogeneous, and this is also reflected in the use of technologies or needs regarding the use of technology. The age and other sociodemographic characteristics of the tandem assistants are not relevant. However, they should feel confident enough in using the smartphone to be able to support the main user.

3.2 Applied Methods

The project's approach is based on a user-centred design [34], where the app is being tested in a real-life setting over several weeks to allow the participants the opportunity to get to know the app and to assess it comprehensively in an everyday setting. Each wave of field testing (pilot 1-3) comprises three dates with face-to-face interviews [35] with the test persons. In addition to the interviews, the study is methodologically based on the think-aloud method [36, 37] and a diary study (paper and pen).

Each of the three face-to-face interviews focuses on different topics: In the first interview, the app is downloaded and installed. One focus here is on questions and problems that arise in this context. The topics of privacy and data protection play a major role here, as the users must give various consents. In addition, the use of the app is explained. Furthermore, it is stated how the test persons generally use their smartphone to understand barriers and needs. The test persons are given the task of trying out the individual functions of the app until the next interview (time span are about 2-3 weeks). The second interview is mainly about usability problems, needs that are not covered by the app and suggestions for improvement. In the third and last interview includes questions about usability again and questions about how the test persons generally obtain information about new apps or digital services.

The interviews are based on semi-structured guidelines and during the interviews the test persons carry out all operating steps as independently as possible and are asked to say out loud everything they do, see, and think. Using the think aloud method, the researchers can understand live which problems and questions are relevant right in the moment of the app use.

Furthermore, the participants are asked to keep a diary (paper & pen method) during the testing period. As soon as they notice something, have problems, ideas for solving problems, questions, and suggestions, they write them down in short form. These notes are always discussed at the beginning of the interviews and flow into the protocols as well. The purpose of the long-term test is for the test persons to get to know the app comprehensively and to try it out. This enables the researchers to develop a deeper understanding of usability issues and user needs. Furthermore, this form of testing can also be used to explore contexts of use and the conditions of acceptance (which framework conditions are central to this).

In addition to usability issues, the focus of Pilot Programme 2 and 3 is strongly on privacy. This applies to the tandem function as well as to online privacy in general. Part of the questionnaire focuses on understanding what concerns the test persons have in this regard and what protection strategies they pursue. All interviews are audio-recorded and selectively transcribed in anonymised form. The selective transcriptions are analysed using qualitative content analysis [38] after each survey wave. Based on this we formed categories relating to privacy issues.

4 Experiences on Online Privacy Behaviours and Needs from a Participants' Perspective

Test participants showed great heterogeneity regarding the extent and content of concerns they uttered. While most participants stated that they were generally not concerned about data privacy, some participants stated that this topic was very important to them. In the following, we present the most striking topics extracted from the interview data relating to online privacy in the context of the *Easierphone* app use, and online privacy in general. The ad-hoc reactions to installation and agreements to terms and conditions and privacy settings can be subsumed under the following categories: Cost-benefit trade-off/privacy calculus, the necessity of trust, coercion and resignation.

Basically, for the installation process of the *Easierphone* app it can be said that the process is largely determined by the Android system requirements. Here, *Easierphone* attempts to make the process as simple as possible while complying to Android guidelines (e.g., asking for various permissions directly on the device). In all real-life interview settings, the test persons and assistants were accompanied or advised by an IAF staff.

4.1 Privacy calculus and the privacy paradox

Most of the test persons in our sample would in fact like to read the general terms and conditions in more detail before they agree, to know more precisely what they are agreeing to. Or in any case, they take the position that that they should actually read them. However, they are not prepared to invest the necessary time or are too impatient for a detailed discussion of the general terms and conditions. One of them stated: "I was going to read it first, but it takes too long, so I think, just agree and skip it" (interview LB12). Also, the phrase, "I don't feel like it" (RD07), was often mentioned. They feel the effort is too great for something that, from their point of view, cannot be avoided anyway. However, a feeling of ambivalence and resignation remains: if you want to use the app, you simply have to accept the terms and conditions. This behaviour relates to the privacy calculus which explains the paradoxical behaviour of the persons as they evaluate potential risks of disclosing private data or agreement against benefit, i.e., here use of the app [32, 33].This behaviour relates to the privacy calculus which explains the paradoxical behaviour of the persons as they evaluate potential risks of disclosing private data or agreement against benefit, i.e., here use of the app [32]. In the explicit context of *Easierphone* testing, the participants also mainly skipped the terms and conditions as they were working or accompanied by IAF staff walking them through the installation process. However, the notification of the *Easierphone* app that the app or data downloaded could be "harmful" irritated a few participants. However, as a cognitive strategy to put aside concerns in the concrete context of testing, test persons often told, "I trust the research project" and it was accepted without deeper scrutiny. One test person even mentioned that they trust the project and, "that everything relating to it [the project] is legally okay" (interview RB05). This relates to findings of Earp, Baumer [31] who examined the effect of a brand name status and found that in general, people

are more open to share or agree to disclose when the company is more well-known. Since the testing was conducted by members of the IAF that is affiliated to the University of applied Sciences Eastern Switzerland, this could have a similar effect in trustworthiness. The statements found in the testing inevitably lead to the next topic of trust in the field of privacy.

The concept of privacy paradox describes the feelings and behaviour of many test persons very well. They describe a contradiction between what they actually do and what they think they should do. The paradoxical behaviour is explained by various factors: there is a lack of willingness to invest the necessary time to read the relevant GTCs or to familiarise themselves with this topic at all. In addition, it is often described that the topic of online privacy is very complex and that the respondents feel overwhelmed by it. This felt lack of knowledge to a feeling of resignation, which in this case does not lead to not using something but to using something despite reservations and question marks. The sometimes-paradoxical behaviours regarding privacy can be understand as resignation to the demands of online privacy but also as cost-benefit trade-off. Some subjects use cognitive and practical strategies to overcome this contradictory situation and feel more secure. For example, they say "I have nothing to hide" (GH07) or "I am not important enough, so no one is interested in my online data" (DG07). Others consistently avoid doing online banking with their mobile phones.

4.2 Necessity of trust

The reactions to the possibility of tandem are often pragmatic. Some already know the principle of "remote access" from the use of the PC (e.g., via TeamViewer) and find it a very practical solution to avoid travel times and regard it is a good thing to transfer this method to the *Easierphone* tandem function. The fact that the main user has control over the access options of the assistant is perceived positively and strengthens the test persons' sense of control over their privacy and make them feel secure when using the tandem functionality. The test persons also see the fact that a tandem partner does not have access to content (chats, emails) but only to interfaces as positive. The ability to view content, however, would be an absolute no-go.

Very few of the test persons see the tandem function as a possibility to provide remote help as critical or a threat to their privacy. The general thrust is that there should be trust in the assisting person, if this trust exists, one has no concerns, if the trust does not exist, one simply does not want to have the person in question as an assistant. Some respondents think that the tandem function is practical but find the asymmetry between the main user and the assisting person problematic: they think that both parties should have equal access to the other person's smartphone.

Regarding the function of AI module within *Easierphone* app, such as activity tracking, the test persons are more critical about the access possibilities of third parties. Several test persons emphasise that they do not want their location to be visible or third parties to see how much they have moved or travelled. A test person here mentioned, "It is nobody's business if I sit on the sofa for a whole day" (EL01). They would feel controlled, their autonomy restricted, and their dignity violated because they no longer have control over their own privacy. Self-tracking per se is not interesting for many of

the test persons. Some use a smartwatch (not connected to the smartphone) and have no need for another tool or emphasise that they don't have their smartphone on them at home and that measured values are therefore not correct anyway. Considering these findings and seeing trust as heuristic in giving agreement to access to another person, or disclose personal information, Scholz and Lubell (1998) [39] this could shorten decision-making procedure.

The view of the assistants (relatives) is clearly differing here: especially if they perceive a relative/partner as fragile (e.g., at risk of falling), the possibility of tracking provides security to them. However, the situation is somewhat different with the emergency call function: here, everyone agrees that location sharing is essential and attractive. Hence, sensitivity to tracking is strongly situational. In general, test persons mentioned during the interviews that active agreement on permissions are necessary as they want to know what the other person, the assistant, knows and has access to.

4.3 Coercion and Resignation

The reflections on concerns, and strategies regarding online privacy in general coincide with those we have in the *Easierphone* app. Some respondents feel safe online because they have "nothing to hide" from a subjective point of view. What is sensitive or could be compromising is highly subjective and can also be interpreted as a mental strategy to mitigate concerns about online privacy by downplaying the importance of their own personal data and disclosure of it. Others think they should protect themselves or read terms and conditions but feel overwhelmed to understand the detailed content and do not want to invest the necessary time. They are of the opinion that the topic of online privacy is too complex and untransparent for laypeople and that they lack the necessary basic knowledge. They feel overwhelmed by the topic, but the benefits of various information, services and apps outweigh their concerns, and they accept everything, but also in the sense of resignation.

Here the privacy paradox appears clearly: Test persons accept terms and conditions although they know they should read the small print including terms and conditions. This behaviour stands in contradiction with their attitude to preferably protect their personal data and not to disclose too much to the public (see also [8]). Nonetheless, a few test persons strictly follow certain strategies to protect their privacy, e.g., in the case of smartphone use: they do not have any bank data stored on their smartphone. The answer to cost-benefit considerations in the context of online privacy is often very pragmatic as one of the citations shows: "I pay the price of getting advertising so that I can use certain apps for free" (interview WG09), or: "I simply accept the terms and conditions so that I can use an app at all" (interview LB12).

In summary, it can be said that privacy concerns are often pushed into the background in favour of simplicity, timesaving, and pragmatism, or are overcome by downplaying them. However, a certain unease or contradictory feelings about online privacy remain. The respondents ultimately feel helpless and impotent when asked how they could overcome these contradictions. The sometimes-paradoxical behaviours relating to privacy can be understand as resignation to the demands of online privacy.

5 Conclusion and Outlook

Easierphone app aims at simplifying smartphone use for older adults and other vulnerable persons. However, usage is not without risk, i.e., disclosure of personal information and acceptance of terms and conditions. Many test persons perceived the basic idea of Easierphone, especially to make the home screen clearer, very positively. However, several participants did mention that it took and still takes time to become familiar with the new layout and functionality of the *Easierphone* app, which also led some participants to preferably use the familiar home screen of their smartphone despite the perceived advantages of *Easierphone*.

We were interested in the behaviours, attitudes, experiences regarding privacy settings and take a closer look at the phenomenon of resignation and the privacy paradox within the research project. The reactions to the topic of online privacy were very heterogeneous. For some, it was generally not a worrying issue, but others expressed reservations but showed resignation and/or paradoxical behaviour. As far as the tandem function was concerned, the conviction of control was greater and the necessary actions to maintain the desired level of privacy towards the assistant were understandable and convertible.

In contrast, it is interesting that what is required by law to protect online privacy (that T&Cs must be shown, and users must give their consent before taking an action) is of little use on a subjective level of being in control over one's privacy in our cases. Test persons were more concerned about what their app assistant or third parties could know about them rather than giving consent for any terms and conditions. It was striking that for example permission granting to access or track routes walked to a known person are more sensitive than maybe also disclosing personal information to a company, here the research institute. This could also be the case because there is a lack of knowledge or willingness, or also lack of experience to deal in detail with the complex issues of online privacy. From a subjective point of view, feelings of coercion, powerlessness and ambivalence are therefore prevalent among the people who have concerns.

This case study shows that experiences and opinions are quite diverse despite a relatively small sample, however, representation was not an aim in the study but to collect and grasp what older adults think about this topic and how behaviour and attitude appear in real life. Privacy and ethical concerns were addressed at several points throughout the pilot testing by the interviewers (e.g., during the installation process of different Easierphone features. While most participants stated that they were generally not concerned about data privacy, some participants stated that this topic was very important to them and that they e.g., try to be vigilant and critical before accepting terms. However, when agreeing to terms of use or grant permission for a function most of the test persons reported to adopt a rather pragmatic approach which can be stated as privacy paradox (i.e., accepting without reading terms (thoroughly). Interesting here is, that test persons distinguished between data that is sensitive (e.g., bank details) and data that they personally perceived as non-confidential (e.g., content of text messages).

To conclude it can be said that the experiences and opinions, attitudes and behaviour of individuals are highly heterogenous. Are there any ways to resolve the privacy paradox and enable older people to have a better sense of control over their online privacy

and thus lower the barrier to digitalisation for older adults? Due to the relatively small sample size (it is part of a larger research project), it is difficult to generalize or even to find similarities among the different test persons. However, the privacy paradox appears frequently appears among them, be it conscious or not. The bridge between real-world privacy strategies and online privacy strategies could ease online privacy strategies, for instance like the assistant app (clear and comprehensible, to what functions the assistant has access and possibility to say yes or no: like closing a door or closing a curtain). Here, further research on what cognitive strategies individual people use to overcome ambivalence, paradoxical feelings, respectively to endure the paradoxical feelings with reference to online privacy is needed.

Acknowledgements

We thank all older participants and their tandem partners without whom we could not have undertaken this research, we would like to extend our sincere thanks for their openness, interest, and valuable time in all interviews in pilot 1 and 2. Further, we thank the European AAL Programme (EU Active Assisted Living Programme) for funding this research project.

References

1. Pew Research Center (2019) Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally. https://www.pewglobal.org/wp-content/uploads/sites/2/2019/02/Pew-Research-Center_Global-Technology-Use-2018_2019-02-05.pdf
2. Seifert A, Martin M, Perrig-Chiello P (2021) Bildungs- und Lernbedürfnisse im Alter: Bericht zur nationalen Befragungsstudie in der Schweiz
3. Seifert A, Ackermann TP, Schelling HR (2020) Digitale Senioren 2020: Nutzung von Informations- und Kommunikationstechnologien durch Personen ab 65 Jahren in der Schweiz
4. Zeissig E-M, Lidynia C, Vervier L et al. (2017) Online Privacy Perceptions of Older Adults. In: Zhou J, Salvendy G (eds) Human Aspects of IT for the Aged Population. Applications, Services and Contexts, vol 10298. Springer International Publishing, Cham, pp 181–200
5. Bartol J, Prevodnik K, Vehovar V et al. (2022) The roles of perceived privacy control, Internet privacy concerns and Internet skills in the direct and indirect Internet uses of older adults: Conceptual integration and empirical testing of a theoretical model. New Media & Society:146144482211227. https://doi.org/10.1177/14614448221122734
6. van Dijk J (1999) The One-Dimensional Network Society of Manuel Castells. New Media & Society 1:127–138. https://doi.org/10.1177/1461444899001001015
7. Kwasny MN, Caine KE, Rogers WA et al. Pricavy and Technology: Folk Definitions and Perspectives. In: CHI 2008 ACM, pp 3290–3296

8. Norberg PA, Horne DR, Horne DA (2007) The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. Journal of Consumer Affairs 41:100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x
9. Rauschnabel PA, He J, Ro YK (2018) Antecedents to the adoption of augmented reality smart glasses: A closer look at privacy risks. Journal of Business Research 92:374–384. https://doi.org/10.1016/j.jbusres.2018.08.008
10. Ghaiumy Anaraky R, Byrne KA, Wisniewski PJ et al. (2021) To Disclose or Not to Disclose: Examining the Privacy Decision-Making Processes of Older vs. Younger Adults. In: Kitamura Y, Quigley A, Isbister K et al. (eds) Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. ACM, New York, NY, USA, pp 1–14
11. Stephanidis C, Salvendy G, Antona M et al. (2019) Seven HCI Grand Challenges. International Journal of Human–Computer Interaction 35:1229–1269. https://doi.org/10.1080/10447318.2019.1619259
12. Elueze I, Quan-Haase A (2018) Privacy Attitudes and Concerns in the Digital Lives of Older Adults: Westin's Privacy Attitude Typology Revisited. American Behavioral Scientist:1372–1391
13. Speck S, Pauli C, Ursprung C et al. (2023) Easierphone: Participative Development of a Senior-Friendly Smartphone Application. In Proceedings of the 9th International Conference on Information and Communication Technologies for Ageing Well and e-Health:199–207
14. Colnago J, Cranor L, Acquisti A (2023) Is There a Reverse Privacy Paradox? An Exploratory Analysis of Gaps Between Privacy Perspectives and Privacy-Seeking Behaviors. PoPETs 2023:455–476. https://doi.org/10.56553/popets-2023-0027
15. Karat C-M, Brodie C, Karat J (2007) Human-Computer Interaction Viewed from the Intersection of Privacy, Security, and Trust. In: Sears A, Jacko J (eds) The Human-Computer Interaction Handbook, vol 20071544. CRC Press, pp 639–658
16. Altman I (1975) The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding. Brooks/Cole Publishing Company, Monterey, California
17. Westin AF (1967) Privacy and freedom. Atheneum, New York
18. Olson JS, Grudin J, Horbitz E A study on preferences on sharing and privacy. In: Proceedings of the SIGCHI Conference on Human factors in Computing Systems, San Jose, California, USA
19. Ludford RJ, Priedhorsky R, Reily K et al. Capturing, sharing, and using local place information. In: Proceedings of the SIGCHI Conference, San Jose, California, USA
20. Bélanger, Crossler (2011) Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Quarterly 35:1017. https://doi.org/10.2307/41409971
21. Li Y (2011) Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework. CAIS 28. https://doi.org/10.17705/1CAIS.02828

22. Smith, Dinev, Xu (2011) Information Privacy Research: An Interdisciplinary Review. MIS Quarterly 35:989. https://doi.org/10.2307/41409970
23. Nissenbaum H (1998) Protecting Privacy in an Information Age: The Problem of Privacy in Public. Law and Philosophy 17:559–596. https://doi.org/10.1023/A:1006184504201
24. Courtney KL (2008) Privacy and senior willingness to adopt smart home information technology in residential care facilities. Methods Inf Med 47:76–81. https://doi.org/10.3414/me9104
25. Tsai H-YS, Shillair R, Cotten SR (2017) Social Support and "Playing Around": An Examination of How Older Adults Acquire Digital Literacy With Tablet Computers. J Appl Gerontol 36:29–55. https://doi.org/10.1177/0733464815609440
26. Kwasny MN, Caine KE, Rogers WA et al. (2008) Privacy and Technology: Folk Definitions and Perspectives. Proc SIGCHI Conf Hum Factor Comput Syst:3291–3296. https://doi.org/10.1145/1358628.1358846
27. Sayre S, Horne DA (2000) Trading Secrets For Savings: How Concerned Are Consumers About Club Cards As a Privacy Threat? ACR North American Advances
28. Phelps J, Nowak G, Ferrell E (2000) Privacy Concerns and Consumer Willingness to Provide Personal Information. Journal of Public Policy & Marketing 19:27–41. https://doi.org/10.1509/jppm.19.1.27.16941
29. Kokolakis S (2017) Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security 64:122–134. https://doi.org/10.1016/j.cose.2015.07.002
30. White TB (2004) Consumer Disclosure and Disclosure Avoidance: A Motivational Framework 14:41–51
31. Earp JB, Baumer D (2003) Innovative web use to learn about consumer behavior and online privacy. Commun ACM 46:81–83. https://doi.org/10.1145/641205.641209
32. Schomakers E-M, Lidynia C, Ziefle M (2019) A Typology of Online Privacy Personalities. J Grid Computing 17:727–747. https://doi.org/10.1007/s10723-019-09500-3
33. Lutz C, Hoffmann CP, Ranzini G (2020) Data capitalism and the user: An exploration of privacy cynicism in Germany. New Media & Society 22:1168–1187. https://doi.org/10.1177/1461444820912544
34. Tullis T, Albert B (2013) Measuring the user experience: Collecting, analyzing, and presenting usability metrics, Second edition. Elsevier/Morgan Kaufmann, Amsterdam, Boston
35. Misoch S (2019) Qualitative Interviews. De Gruyter
36. Nørgaard M, Hornbæk K (2006) What do usability evaluators do in practice? In: Carroll JM, Bødker S, Coughlin J (eds) Proceedings of the 6th conference on Designing Interactive systems. ACM, New York, NY, USA, pp 209–218
37. Ericsson KA, Simon HA (1993) Protocol Analysis. The MIT Press
38. Mayring P (2000) Qualitative Content Analysis [28 paragraphs]. Forum Qualitative Sozialforschung / Forum: Qualitative Social Research,

39. Scholz JT, Lubell M (1998) Trust and Taxpaying: Testing the Heuristic Approach to Collective Action. American Journal of Political Science 42:398. https://doi.org/10.2307/2991764