Original Paper

Data Privacy Concerns Using mHealth Apps and Smart Speakers: Comparative Interview Study Among Mature Adults

Tanja Schroeder[1,2], BA, MA; Maximilian Haug[2], BEng, MSc; Heiko Gewald[2], BSc, MBA, EMBSc, PhD

[1]Centre for Health Systems and Safety Research, Australian Institute of Health Innovation, Macquarie University, Sydney, Australia

[2]Center for Research on Service Sciences, Neu-Ulm University of Applied Sciences, Neu-Ulm, Germany

Corresponding Author:
Tanja Schroeder, BA, MA
Centre for Health Systems and Safety Research
Australian Institute of Health Innovation
Macquarie University
75 Talavera Road
Sydney, NSW 2109
Australia
Phone: 61 2 9850 ext 6281
Email: tanja.schroeder@hdr.mq.edu.au

Abstract

Background: New technologies such as mobile health (mHealth) apps and smart speakers make intensive use of sensitive personal data. Users are typically aware of this and express concerns about their data privacy. However, many people use these technologies although they think their data are not well protected. This raises specific concerns for sensitive health data.

Objective: This study aimed to contribute to a better understanding of data privacy concerns of mature adults using new technologies and provide insights into their data privacy expectations and associated risks and the corresponding actions of users in 2 different data contexts: mHealth apps and smart speakers.

Methods: This exploratory research adopted a qualitative approach, engaging with 20 mature adults (aged >45 years). In a 6-month test period, 10 (50%) participants used a smart speaker and 10 (50%) participants used an mHealth app. In interviews conducted before and after the test period, we assessed the influence of data privacy concerns on technology acceptance, use behavior, and continued use intention.

Results: Our results show that although participants are generally aware of the need to protect their data privacy, they accept the risk of misuse of their private data when using the technology. Surprisingly, the most frequently stated risk was not the misuse of personal health data but the fear of receiving more personalized advertisements. Similarly, surprisingly, our results indicate that participants value recorded verbal data higher than personal health data.

Conclusions: Older adults are initially concerned about risks to their data privacy associated with using data-intensive technologies, but those concerns diminish fairly quickly, culminating in resignation. We find that participants do not differentiate between risky behaviors, depending on the type of private data used by different technologies.

(JMIR Form Res 2022;6(6):e28025) doi: 10.2196/28025

KEYWORDS

data privacy concerns; privacy paradox; mHealth app; smart speaker; mature adults; smartphone

Introduction

Overview

A mobile health (mHealth) app is a specific type of digital health app that uses mobile devices such as smartphones and tablets that are already integrated into daily lives of people. People use mHealth apps to monitor their health or access medical information or assistance through wireless mobile devices such as smartphones and portable monitoring devices [1]. Similarly, mHealth apps enable health care providers to monitor certain user activities and behaviors so that they can provide personalized health care advice. Other technologies can also be used to support personalized health care support. For example, smart speakers with artificial intelligence–operated assistants that help users more easily access information or control other devices via their voice can be used for this purpose [2,3].

Although smart speakers are often used for everyday activities, such as playing music, setting a timer, or hearing a weather report, they can also be used to remind users to take their medication or answer health-related questions. Smart speakers collect and process a variety of private information and are typically used in private environments. Because a smart speaker must be able to recognize the voice activation keyword at any time, its microphone's default status is active. Therefore, many people associate smart speakers with involuntary personal information disclosure [4].

The increasing use of digital and mobile technologies, combined with the need for personalized and cost-efficient health care, has fostered the emergence of mHealth technologies. Such technologies have many potential health care benefits, such as the ability to monitor users' health status continuously and remotely, increased diagnostic accuracy, earlier awareness of new problems, lower health care costs, greater availability of health care to people living in remote areas, and improved doctor-patient communications.

Despite these potential benefits, the sensitivity of individuals' private data collected and recorded by these digital apps raises concerns about the privacy of this information [5,6]. For example, some potential users want to control what people in their private environment, such as family members, know about their health status, perhaps because they fear being judged, reprimanded, discriminated against, or even penalized for their physical and health status [7]. Some people may not want to take care of their family members because of their current health status [7,8]. The fear of social stigmatism is another reason people may not want others to know their health status [8]. This may apply to physical or mental disabilities, mental illnesses, or certain diseases such as HIV and Alzheimer [8,9].

In this study, we define *privacy* as the right of individuals, groups, or institutions to determine when, how, and to what extent information about them is shared with others [10]. Privacy is a subjective concept linked to an individual's perception of what constitutes a threat to their personal property or physical or moral integrity, depending on cultural aspects and sociodemographic issues [11]. Users' perspectives on interactions and communications influence their data privacy–related decisions on a range of privacy issues, including technical issues such as regulating visibility in social networks and using smartphone apps that collect confidential data [12].

Most extant data privacy literature focusing on mHealth deals with the technical aspects of privacy, such as the level of security of information transmitted over mobile networks and stored on a device or in a cloud service needed to prevent unauthorized access to a patient's information [8,13-15]. However, privacy is not only a technical issue. For example, the collaborative use of mHealth apps for shared care management imposes other privacy requirements related to human factors, such as the wishes and preferences of the user when exchanging health information with authorized institutions and external persons such as professional health care providers [16].

Extant research shows that privacy concerns are a major inhibitor of the adoption and use of both mHealth apps and smart speakers [4,17]. Because the 2 technologies access different types of sensitive personal data, potential users may have different privacy concerns regarding each technology. To investigate this issue, we posed the following research questions (RQs):

1. RQ1: What privacy concerns do potential users associate with mHealth apps and smart speakers?
2. RQ2: What data privacy–related risks do potential users attribute to the use of mHealth apps and smart speakers?
3. RQ3: What privacy-related issues lead to rejection of mHealth apps and smart speakers?

Although the use of smart speakers is roughly equal among *mature adults*, which we define as people who are aged >45 years and adults aged <45 years [18], extant research shows that mobile apps for health care purposes are most commonly used by mature adults [19]. Because this study addresses both technologies, we focus on the mature adult user group, providing 50% (10/20) of the participants with a smart speaker and 50% (10/20) of the participants with an mHealth app to use in a 6-month testing phase. All the participants were interviewed before and after the testing phase.

Background

One of the main reasons why people are reluctant to use mHealth apps is concerns about the security and privacy of their health-related data [20-23]. Users often do not know what kind of data mHealth apps collect and store and who can access data entered manually or collected by sensors and for what purposes [20,24]. Studies show that users have greater security and privacy concerns about mHealth apps that focus on issues associated with stigmatization, discrimination, or social isolation, such as sexually transmitted diseases, sexual orientation, and mental illnesses [25-29]. Considering that millions of patients' health data have been compromised through hacking or other incidents in recent years, these concerns are valid [30]. Despite private data security breaches, few mHealth apps have security features that adequately protect users' private health data [31-33].

Privacy Theories

Extant research has not yet fully explored the specific role of privacy concerns in the acceptance and use of technology. The privacy calculus theory [34,35] and the so-called *privacy paradox* [36] are central concepts in privacy research. They illustrate the ambivalent influence of privacy on behavior.

The privacy calculus theory assumes that individuals engage cognitively to weigh the perceived costs and benefits of a behavior [34,35]. If the benefits outweigh the potential harm that privacy abuse can induce, individuals engage with the technology. However, this view is partly challenged by the privacy paradox, a phenomenon in which individuals engage with a technology even though the privacy concerns they associate with using the technology outweigh the anticipated benefits of using it [36,37]. Although both phenomena are well documented in practice, technology adoption scholars have yet to explain this conundrum [38].

Privacy Research

Computer system privacy has long been a concern. In 1969, a study by Hoffman [39] discussed strategies for user access control and data protection, emphasizing the need to weigh the efficiency benefits of storing personal information against the risks of third-party access to such information. The study examined legal and administrative safeguards to protect sensitive information on computers and evaluated the technical solutions available at the time.

More recently, a study by Barth and De Jong [40] focused on privacy-related human factors. They conducted a systematic literature review to understand the web-based privacy paradox, where users indicate great concern about the privacy of their personal information but do very little to protect such data. The authors identified 35 theoretical approaches to decision-making and identified different perspectives on the paradox. Specifically, they discuss the decision-making process after rational or irrational risk-benefit calculations in the specific context of the privacy paradox.

Pavlou [41] described the data protection paradox in his privacy briefings as a phenomenon in which individuals express strong concerns about their privacy but behave in a way that contradicts these concerns. For example, some consumers still share their personal information despite privacy concerns. Even after considering the user perspective, Aïmeur [42] addressed the question of how to achieve a good compromise between privacy and user personalization. He mentioned that an increasing number of users can only control their data by fine-tuning the app settings. The author also argued that mHealth would benefit significantly if users had direct control over when, where, and with whom their personal data were shared.

Privacy-Personalization Paradox

Varshney [43] described privacy as the right of a group or individual to isolate or retain information about themselves. Personalization technologies offer users a wide range of services from which to choose but also require users to disclose more personal information, which may raise privacy concerns [44]. This has been compounded by the emergence of smartphones that can capture personal information more accurately [45]. For example, health care counseling provided via mobile platforms can reduce the need for personal interaction, but app users must then share information relevant to their health, such as health status, preferences, and lifestyle, as well as their telephone number with service providers to use personalized health care counseling services that overcome geographic barriers and save time. This, in turn, raises privacy concerns regarding the collection of sensitive consumer information: a technological paradox [46]. Although consumers want personalized services, they are reluctant to disclose personal information and want to disclose as little information as possible.

Demographics

Demographic differences between potential consumers are linked to behavioral intentions [47-50]. Some studies have focused on age differences in technology adoption, suggesting that there are differences in intentional behavior among different age groups [51]. However, Featherman and Pavlou [52] found that the validity of theoretical constructs, including models of health behavior change, is not well documented at all life stages. Most scholars agree that as people age, their physical and mental activities change, which affects their health status and decision-making [53]. Researchers have recently recognized that studying age differences in behavioral intention in the health context is both useful and essential. Ziefle and Röcker [54] found that age differences played an important role in the acceptance of health-related technologies. Similarly, Sintonen and Immonen [55] found that older participants' intention to adopt technology varies over time and according to the service provided, whereas a study by Guo et al [56] found that *dark-side* constructs influence older participants' intention to adopt mHealth services.

Methods

Recruitment and Demographics

This is an exploratory qualitative study with 20 participants divided into 2 groups. Semistructured interviews were conducted between October 2019 and April 2020, in southern Germany. Each group consisted of 10 participants aged between 46 and 80 years. Group A participants used smart speakers with Amazon Alexa technology, and group B participants used a self-provided mHealth app on their Android smartphone. Both technologies were provided to the participants free of charge.

Smart speakers are voice-controlled, enabling users to play music or news, access information, place telephone calls, and perform other tasks via voice commands. The smart speaker is activated by speaking a predefined voice command. The smart speakers have several levels of built-in privacy measures. For example, a microphone can be deactivated by pushing a button that interrupts its power supply. Users also retain full control over voice recordings. Users can also control whether, when, and which voice recordings are accessed or accessible by third parties through the internet.

The mHealth app incorporates a health diary that users can use to track their daily health status, water intake, and other health-related information. This app is mainly intended to make daily life easier for older people. Referring to a digital health diary should allow health care providers to collect relevant information more effectively and quickly and make the process less burdensome for older people. In addition, it aims to prevent a decline in cognitive performance. Using the *My values* feature, users can choose from a wide range of functions within the app, including body temperature, blood pressure, heart rate, blood glucose levels, and weight. Users can query the recorded data using various time intervals. In addition, users can activate a push notification function to receive reminders to enter current measurement values.

The participants were recruited in southern Germany through flyers and posters in senior citizen centers and postings on social media. Participation was strictly voluntary, and no incentives were provided. All participants interviewed were informed of the research team's data protection arrangements and signed a document to this effect in full compliance with the European Union data protection regulations, the General Data Protection

Regulation (GDPR). Participants interested in taking part in the study were given a participant information sheet and an informed consent form detailing the participation requirements in advance, with the option to have the form explained if necessary. Participants signed and returned the form, indicating their informed consent. The consent forms were retained and stored securely as a record of informed consent. Participants could withdraw from the interviews at any time during the study if they no longer wanted to be included. Furthermore, the researchers were available to answer questions at any time. The research group saved all participant data anonymously and retained all written and audio materials collected during the interviews until the end of the data retention period. All project data are stored electronically on secure password-protected servers and accessible only by designated and approved project team members. All the data will be destroyed at the end of the data retention period.

Table 1 provides demographic information of the participants.

All participants were considered IT affine, demonstrating interest in digital technologies such as smartphones, tablets, PCs, smart watches, or smart speakers. All participants actively used a smartphone and at least one social media service regularly and demonstrated at least an average internet use intensity for their age group. All interviewees were able to install and set up a smart speaker or an mHealth app with little or no assistance.

Table 1. Demographics of the participants (N=20).

Participant group and informant	Age (years)	Gender
Group A		
A1	56	Female
A2	59	Female
A3	54	Female
A4	48	Female
A5	49	Male
A6	70	Male
A7	68	Male
A8	56	Male
A9	54	Male
A10	46	Male
Group B		
B1	52	Male
B2	50	Male
B3	55	Female
B4	60	Female
B5	56	Female
B6	61	Female
B7	54	Female
B8	52	Female
B9	80	Male
B10	51	Male

Data-Gathering Process

The study was structured into three phases: (1) before, (2) during, and (3) after testing the respective technologies.

Phase 1 began with participant recruitment and ended with the delivery of the technology to be tested. This phase included the first conversation to give participants detailed information about the study approach and timeline, collect demographic data, interview all participants about their expectations toward using new technology and their concerns about protecting their private data, and ask participants who would test the mHealth app about their experiences in preventive health care. We also asked specific questions about privacy concerns related to the technology tested in our study.

Phase 2 started with the delivery of the technology and ended when the technology was returned (smart speaker) or uninstalled (mHealth app). This 6-month phase gave participants ample time to test the technology thoroughly. During this phase, research assistants (MH, Jennifer Klaus, and Jaro Lanza) were available to help if participants encountered difficulties using the technology.

Phase 3 started when the technology was returned or uninstalled and ended when all data were collected and ready to be

analyzed. During this phase, we conducted posttest interviews with each participant to discuss their use behavior, observations, problems, and concerns. We paid special attention to how their assessment of data privacy concerns changed over time and how this influenced their intention to continue using the technology.

Interview Structure and Data Analysis Method

In phases 1 and 3, we conducted individual semistructured interviews with each participant, following an interview guide and drawing on a list of topics and specific questions. We posed open-ended questions that allowed the respondents to explore their experiences and views. The interview guide helped focus the interview and ensured the comparability of data collected among multiple participants in various interview settings and by different researchers. The interview process was systematic and comprehensive, but the interviewer was free to follow up on issues of greater interest or importance to the participant during the interview by adapting preformulated questions ad hoc to gain a deeper and more holistic understanding of the participants' perspectives and perceptions.

As the aim of this study was to understand the relationships among privacy concerns, risk perception, and use behavior in the technology-use context, we focused principally on privacy concerns, the impact of data misuse, and termination of use.

The 10 pretest and the 10 posttest interviews lasted 15 to 60 minutes each (average 35, SD 15.59 minutes) and were conducted face to face or via telephone or videoconference. The interviews were conducted in German and recorded, transcribed, and coded using an open coding approach using NVivo (version 10; QSR International) software independently by 2 research team members (TS and MH). The research team coded the data parallel to data collection. Subsequently, the data were triangulated according to the recommendations by Miles et al [57] and Flick [58]. The analysis took an inductive and interpretative approach. The inductive approach is a systematic procedure for analyzing qualitative data in which the analysis is guided by specific objectives [59].

In the second round of analysis, the codes from the individual interviews were correlated [57] to cast light on the specific characteristics of these topics and the influence of these factors in the context of the two technologies.

Ethics Approval

This study did not require ethical approval according to the guideline of the applicable Ethics Committee of the Bavarian Universities (Gemeinsame Ethikkommision der Hochschulen Bayerns [60]), as no risks or harm to the participants were expected and the basic ethical principles were not violated. All participants received a participant information and consent form explaining the requirements for participation, with the option to have the form explained to them if needed and gave their verbal consent as a sign of informed consent if they were willing to participate at the time of the interview. They were also given the opportunity to complete and sign the participant consent form to indicate their agreement to the interview being conducted.

Results

Overview

The pretest interviews focused on participants' general expectations regarding the technology, as well as their privacy concerns and expected risks associated with using the technology. The posttest interviews focused generally on how the informants had used the technology during the test phase, specifically on whether their privacy concerns and their perceptions of the risks changed during the 6-month testing phase, and if the intention to continue using the technology.

To better segregate the 2 different types of data used by the technologies we refer to "health data" for the data used by the mHealth app which predominantly consist of the participant's health status or well-being information and "personal data" for the data collected by the smart speaker, which comprises mainly intended and unintended speech, as well as the information transmitted when the user gives commands to the speaker.

Privacy Concerns

Overview

Individuals' privacy concerns are shaped and influenced by many factors, such as personal experiences, media coverage, and the social environment [61-64]. Therefore, it is essential to understand participants' perceptions of individual data privacy–related issues to be able to classify their statements and derive results. To better understand how privacy concerns impact the use of smart speakers and mHealth apps, we asked participants directly about their privacy concerns and perceptions of privacy-related issues.

It should be noted that some of the participants testing a smart speaker had previous experience using them, were more aware of privacy-related issues associated with them, and had already formed opinions about the risks and benefits of using them. In contrast, the participants testing a smart speaker for the first time had a basic understanding of the technology but were less aware of the privacy-related issues associated with them and did not know what to expect. None of the participants testing the mHealth app had prior experience of using an mHealth app.

The following 2 sections present our core findings, supported by exemplary quotations translated from the German original. The alphanumeric codes after each quotation refer to the quoted participants and other participants who expressed similar viewpoints.

Smart Speakers

Participants commonly expressed awareness of privacy issues associated with using a smart speaker:

> *I would say that I have a high level of data protection awareness. [...] I am very aware that the data that I enter on the Internet or that is processed via the Internet can be accessed by providers and misused.* [A8; A10]

Most (8/10, 80%) participants expressed concerns regarding data protection:

> *No, I do not think that the data is secure.* [A2; A5; A8; A9]
>
> *I do not think the data is secure. The data is recorded and stored, and once the data is on the Internet, it is not safe for me either.* [A3]

In addition, most (6/10, 60%) participants articulated some degree of concern that their data would be stored somewhere unknown and used without their permission. This illustrates a general tendency of users to doubt that their data will be protected:

> *I think there are loopholes and problems, and that data is not protected adequately.* [A1; A5; A6; A7; A8; A9]

Most (6/10, 60%) participants expressed resignations. Although they were concerned about their privacy, they also recognized that if they wish to participate in web-based activities or use certain apps, they must accept the terms of use and may lose control over their data. Many eventually decide to use an app, while maintaining some degree of privacy awareness:

> *Let me put it like this: I have a rather low data protection awareness. I ignore who can process my data.* [A1; A2]
>
> *I would describe my data protection awareness as not consistent enough to protect my data.* [A3; A5]
>
> *I take care of my data. Nevertheless, I think that I cannot really influence or intervene and determine who gets my data. As soon as I download and use an app, I have to agree to the terms of use.* [A6; A7]

However, some (2/10, 20%) participants expressed no concerns at all. A prominent issue is confidence in the manufacturer (in this case, Amazon).

> *The way I see it, as long as I feel sure, I will use the device; if trust is no longer there, then I think that I will no longer use the device.* [A6]
>
> *I have great confidence in Amazon that my data will be stored securely.* [A10]

In summary, our results show that most (8/10, 80%) participants have privacy concerns about using a smart speaker and are not sure what happens to their data. However, the participants did not fear monetary loss or reputational injury. We found that participants were willing to suppress their own data protection concerns to use the device and justified putting aside any lack of trust in the provider.

mHealth App

In the group using the mHealth app, participants' views on privacy and data protection concerns were split—half (5/10, 50%) of the participants said that they were not worried or concerned about the privacy of their personal data:

> *They cannot do much with my data anyway because I am an ordinary person. [...] what I use or look at or, how should I say it, [...] that is what every human being does, to put it like that.* [B1]
>
> *No. I've got nothing to hide.* [B5]
>
> *Not at all, actually. [...] And I have nothing to hide. But I am not afraid that this will end up anywhere.* [B9]

In contrast, (4/10, 40%) of the participants were concerned about data protection and privacy:

> *Yes, I have become very concerned. [...] Because the different sites are obviously not safe and a lot of data is collected about you, you do not know anything about it. Of course, it is great to have computers here, if you get a lot of information, but there is also a certain potential to become dependent on them, and as I said, I see a problem with surveillance and abuse.* [B6]

The most frequently mentioned concerns include surveillance, abuse, and use of your data against you:

> *Partly yes, but I mean I know what I can write about on my smartphone and what I cannot say. [...] I think you have to have restrictions about that. [...] I am just careful what I [...] write. [...] What would be on a postcard, you would write like that, I would say.* [B10]

Overall, our results show that participants vary in terms of their data protection concerns and how they engaged with data privacy, specifically with regard to using a smart speaker or an mHealth app.

Smart Speaker Versus mHealth App

Our results indicate that attitudes vary depending on the device and how information is captured or entered. As expected, participants were most sensitive to personal data. Somewhat surprisingly, our results indicate that participants are more concerned about personal speech recorded by a smart speaker than about personal health data entered into an mHealth app.

Data Misuse

To better understand the degree to which participants' concerns about data misuse are justified, we inquired about the perceived ramifications of misuse of data collected via the smart speaker or eHealth app.

Smart Speaker

Most (9/10, 90%) participants testing smart speakers associate smart speaker data misuse with personalized advertisements. Some have linked it to profiling, monetary loss, and data loss:

> *I think that my data will be used for advertisement. I mean that they sell my data to agencies to show me ads at the right time.* [A7; A2]
>
> *They could take money from my bank account. Alternatively, they will spam me with e-mails or ads.* [A4; A10]

mHealth App

Of the 7 participants who reported believing that their data were sold to unknown third parties, 3 (43%) assumed that their data were stored on unknown servers by companies such as Google. A few (3/10, 30%) participants had never considered this issue:

> *They trade our data, the data is sold, and that is well known. And yes, it is used to send advertisements to advertising companies.* [B8]
>
> *The data is just sitting around in some archive. Or someone can buy it. No idea. I have not really thought about it.* [B4]

Some (2/10, 20%) participants raised concerns about potential negative implications for existing insurance policies or apps for new insurance policies because of chronic or serious illnesses:

> *Yes, I do not see any problems there now, because my health is good. I can well imagine that others might have a problem because they think if everyone knows that I have trouble taking out an insurance policy or get offered worse conditions, but theoretically this is already the case.* [B3]
>
> *No, not really. I no longer have a problem with any health insurance companies at my age. I am privately insured so of course nothing will change. And I do not need to take out large insurance policies anymore, but if I were younger, I would be much more aware of the fact that the data might be misused.* [B6]

These statements indicate a much deeper understanding of the potential implications of data abuse in the health care context, including direct monetary damage. However, the risks described did not result in grave concerns or technology rejection among the respondents.

Termination of Use

No participant in either group stopped using the technology or intended to stop using the technology after the test because of data privacy concerns, and we observed no increase in data privacy concerns over time. Across the board, participants assumed that data were collected to enable personalized advertisements, which did not represent a salient enough risk to participants to motivate the termination of use.

Smart Speakers

Participants testing smart speakers reported several data privacy issues that would hypothetically motivate them to stop using it, including privacy violations, data leaks, and eavesdropping:

> *I would stop using it if I myself were affected, such that people could openly access my data.* [P5; P7; P9]
>
> *If I suddenly got advertising/promotional mails or phone calls, I would not use it anymore.* [P1; P3; P4; P8]

However, such hypothetical concerns and risks did not motivate participants to discontinue using technology. Rather, participants would have to experience an incident personally to trigger actual termination of use.

mHealth App

Participants testing the mHealth app reported that no data privacy issues would hypothetically motivate them to stop using the app:

> *No, not at all.* [B3]
>
> *Not significantly.* [B9]

Interestingly, none of the participants were seriously concerned about data privacy and the protection of their health data when using the mHealth app.

Discussion

Principal Findings

This study aimed to determine whether data privacy is perceived differently for different data-intensive technologies. By comparing 2 groups of mature adult users, we assess how the impact of privacy concerns, such as data protection concerns and risks, on technology use and discontinuation differs depending on the technology.

In both user groups, none of the participants stopped using the technology, despite privacy concerns. This is in line with the widely discussed privacy paradox [36], which states that individuals engage with technology even when they associate it with potential privacy loss issues. This phenomenon has been observed in social media, e-commerce, and mobile apps [45,65,66]. A likely driver of this paradoxical behavior is that the perceived immediate benefits of using a technology outweigh its potential, hypothetical, future risks [67]. Our results also indicate that this applies to health data privacy risks as well. In both user groups, participants expressed widespread resignation that choosing to use the technology comes at the cost of a greater risk of potential loss of data privacy.

Surprisingly, our results also show that people do not associate greater risk with personal health data collected by an mHealth app than with spoken words recorded by smart speakers. Because personal health data are highly sensitive and provide deep insights into individuals, one would expect users to be more concerned about protecting their privacy [68]. One possible explanation is that discrete data entered manually, consciously, and willingly, such as health status data in an mHealth app, are easier to control than impromptu utterances spoken all day long in a private setting. Regardless, our results call into question whether users of information technology, who require personal information distinguish between the data types collected by various devices and whether users fully understand the financial and personal ramifications of data abuse beyond personalized advertising.

In contrast with the mHealth app, which only passively receives data entries, a smart speaker may be perceived as invasively and nontransparently intruding into the private space. Indeed, several smart speak testers referred to the device's constant *listening* for the activation keyword as *spying* in the pretest interviews. However, no participants used this term in the posttest interviews after the 6-month test phase. This may indicate that they perceived greater risk to their privacy in the preadoption than in the postadoption phases, as they are commonly referred to in technology adoption research [69,70].

Our results provide initial indications of a potential decline in the perceived fear of loss of private health data with increasing age. Several older participants stated that no one would be interested in their health data; therefore, privacy breaches posed no threat to them. Further research is needed to discern consistent patterns of age-related differences.

Implications for Research

This exploratory research contributes to research on how data privacy concerns influence the intended and continuous use of data-intensive technologies, specifically mHealth apps and smart speakers. Investigations into the specific perceptions and resulting behaviors of mature adults in privacy research are scarce, and scholars still have only a rudimentary understanding of how older people's engagement with technology is influenced by privacy-related issues and concerns. This is especially important, as mHealth apps and voice-activated assistants gain increasing importance in providing health care–related services to mature and older adults [71].

Our findings have 4 major implications for research. As our findings are based on an exploratory qualitative research method, their implications do not aim to be representative of all mature adults but provide a basis for further research to investigate quantitatively.

First, our findings indicated that mature adults' self-reported privacy concerns did not directly influence their actual use behavior once they had adopted a data-intensive technology. This finding is consistent with the privacy paradox [36]. Participants frequently entered a state of resignation, acknowledging that choosing to use the technology requires them to accept the potential loss of data privacy.

Second, our results indicated that mature adults sometimes view their personal data indiscriminately. Even when participants were aware of the risks of data misuse, they articulated that the risks did not affect them personally or would not manifest themselves in their case. The risk that participants mentioned the most was receiving more personalized advertisements. In fact, participants valued protecting their general personal data more than protecting their personal health data, positing that they were not worthwhile targets of health data theft. This is concerning, especially considering recent health-related data hacks [72].

Third, our results pointed to age as a moderating factor in the perception of data privacy, risk assessment, and the subsequent application of privacy calculus. Several older participants articulated that their data privacy–related risks were low because of their age. Lee et al [73] showed that the tendency to discount future risks was prevalent among younger people. Our study indicated that this influence may be more substantial for older people who, according to our study, lack motivation to engage with how their personal data will be treated and are, therefore, more willing to disclose their personal data.

Finally, somewhat surprisingly, we found that data type did not significantly affect how participants perceive data privacy issues. We expected that participants would be more concerned about protecting the privacy of their personal health data than about protecting more general personal information. However, participants initially considered all personal data as equally worthy of protection, possibly insufficiently understanding the ramifications of data abuse and not reliably distinguishing between different types of data processed through different devices. Further research is needed on the role of data types in technology users' privacy calculus, as current privacy models do not distinguish among different types of data or consider individuals' perceptions of different types of data.

Limitations and Further Research

This study is exploratory in nature; therefore, our results are not generalizable to all mature adults and all data-intensive technologies. Furthermore, all participants were recruited in the south of Germany and thus shared a certain cultural background. As with every qualitative study, this study is subject to potential bias from the research team and potentially influenced by social desirability bias among participants.

Our findings suggest several avenues for further research. Specifically, we call for further research on how the act of *resignation* manifests in users' privacy calculus as an acceptable price to pay for using a certain technology. Further research is also needed to understand what drives people to value certain types of personal data more than others, which, in our case, is valuing general personal data used to personalize advertising more than personal health data, which can be misused with grave consequences. Finally, a cross-generational study is required to assess the influence of age on data privacy concerns and technology adoption.

Conclusions

Research on how mature adults' data privacy concerns influence their use of data-intensive technology is scarce, despite reports of data hacks and leaks and eavesdropping on prominent technologies and the sensitive nature of personal health data. The results of our exploratory research analyzing interviews with 20 mature adult users of data-intensive technologies reveals that although participants self-reported initial data privacy concerns, they did not value the risks high enough to discontinue using the data-intensive technologies in focus. Rather, they expressed widespread resignation that choosing to use the technology means accepting the risk of loss of data privacy. This fatalistic surrender, combined with evidence that participants valued their general personal data more than their personal health data, is a cause for concern about the security of personal data among technology users of this generation.

Conflicts of Interest

None declared.

References

1. Global diffusion of eHealth: making universal health coverage achievable: report of the third global survey on eHealth. World Health Organization. 2017. URL: https://apps.who.int/iris/handle/10665/252529 [accessed 2012-11-20]

2. Park K, Park Y, Lee J, Ahn JH, Kim D. Alexa, Tell Me More! The effectiveness of advertisements through smart speakers. Int J Electron Commer 2022 Feb 16;26(1):3-24. [doi: 10.1080/10864415.2021.2010003]
3. Kim S. Exploring how older adults use a smart speaker-based voice assistant in their first interactions: qualitative study. JMIR Mhealth Uhealth 2021 Jan 13;9(1):e20427 [FREE Full text] [doi: 10.2196/20427] [Medline: 33439130]
4. Malkin N, Deatrick J, Tong A, Wijesekera P, Egelman S, Wagner D. Privacy attitudes of smart speaker users. Proc Priv Enh Technol 2019;2019(4):250-271. [doi: 10.2478/popets-2019-0068]
5. Boulos MN, Brewer AC, Karimkhani C, Buller DB, Dellavalle RP. Mobile medical and health apps: state of the art, concerns, regulatory control and certification. Online J Public Health Inform 2014 Feb 5;5(3):229 [FREE Full text] [doi: 10.5210/ojphi.v5i3.4814] [Medline: 24683442]
6. Dehling T, Gao F, Schneider S, Sunyaev A. Exploring the far side of mobile health: information security and privacy of mobile health apps on iOS and Android. JMIR Mhealth Uhealth 2015 Jan 19;3(1):e8 [FREE Full text] [doi: 10.2196/mhealth.3672] [Medline: 25599627]
7. Prasad A, Sorber J, Stablein T, Anthony D, Kotz D. Understanding sharing preferences and behavior for mHealth devices. In: Proceedings of the 2012 ACM Workshop on Privacy in the Electronic Society. 2012 Presented at: WPES '12; October 15, 2012; Raleigh, NC, USA p. 117-128. [doi: 10.1145/2381966.2381983]
8. Silva W, Sacramento C, Silva E, Garcia AC, Leal Ferreira SB. Health information, human factors and privacy issues in mobile health applications. In: Proceedings of the 53rd Hawaii International Conference on System Sciences. 2020 Presented at: HICSS '20; January 7-10, 2020; Maui, HI, USA p. 3429-3438. [doi: 10.24251/hicss.2020.420]
9. Koffi B, Yazdanmehr A, Mahapatra R. Mobile Health Privacy Concerns - A Systematic Review. In: Proceedings of the 24th Americas' Conference on Information Systems. 2018 Presented at: AMCIS '18; August 16-18, 2018; New Orleans, LA, USA p. 25 URL: https://aisel.aisnet.org/amcis2018/Health/Presentations/25
10. Westin AF. Privacy and freedom. Wash Lee L Rev 1968 Mar 1;25(1):165-170.
11. Dupuis MJ, Crossler RE, Endicott-Popovsky B. Measuring the human factor in information security and privacy. In: Proceedings of the 49th Hawaii International Conference on System Sciences. 2016 Presented at: HICSS '16; January 5-8, 2016; Koloa, HI, USA p. 3676-3685. [doi: 10.1109/hicss.2016.459]
12. Acquisti A, Adjerid I, Balebako R, Brandimarte L, Cranor LF, Komanduri S, et al. Nudges for privacy and security: understanding and assisting users' choices online. ACM Comput Surv 2018 May 31;50(3):1-41. [doi: 10.1145/3054926]
13. Sharma S, Chen K, Sheth AP. Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems. IEEE Internet Comput 2018 Mar;22(2):42-51. [doi: 10.1109/mic.2018.112102519]
14. Saleheen N, Chakraborty S, Ali N, Mahbubur Rahman M, Hossain SM, Bari R, et al. mSieve: differential behavioral privacy in time series of mobile sensor data. Proc ACM Int Conf Ubiquitous Comput 2016 Sep;2016:706-717 [FREE Full text] [doi: 10.1145/2971648.2971753] [Medline: 28058408]
15. Silva BM, Rodrigues JJ, Canelo F, Lopes IC, Zhou L. A data encryption solution for mobile health apps in cooperation environments. J Med Internet Res 2013 Apr 25;15(4):e66 [FREE Full text] [doi: 10.2196/jmir.2498] [Medline: 23624056]
16. Avancha S, Baxi A, Kotz D. Privacy in mobile technology for personal healthcare. ACM Comput Surv 2012 Nov;45(1):1-54. [doi: 10.1145/2379776.2379779]
17. Zhou L, Bao J, Watzlaf V, Parmanto B. Barriers to and facilitators of the use of mobile health apps from a security perspective: mixed-methods study. JMIR Mhealth Uhealth 2019 Apr 16;7(4):e11223 [FREE Full text] [doi: 10.2196/11223] [Medline: 30990458]
18. Kinsella B. Voice Assistant Demographic Data – Young Consumers More Likely to Own Smart Speakers While Over 60 Bias Toward Alexa and Siri. Voice Bot AI. 2019 Jun 21. URL: https://voicebot.ai/2019/06/21/voice-assistant-demographic-data-young-consumers-more-likely-to-own-smart-speakers-while-over-60-bias-toward-alexa-and-siri/ [accessed 2021-05-05]
19. Rasche P, Wille M, Bröhl C, Theis S, Schäfer K, Knobe M, et al. Prevalence of health app use among older adults in Germany: national survey. JMIR Mhealth Uhealth 2018 Jan 23;6(1):e26 [FREE Full text] [doi: 10.2196/mhealth.8619] [Medline: 29362211]
20. Atienza AA, Zarcadoolas C, Vaughon W, Hughes P, Patel V, Chou WY, et al. Consumer attitudes and perceptions on mHealth privacy and security: findings from a mixed-methods study. J Health Commun 2015;20(6):673-679. [doi: 10.1080/10810730.2015.1018560] [Medline: 25868685]
21. Kao CK, Liebovitz DM. Consumer mobile health apps: current state, barriers, and future directions. PM R 2017 May;9(5S):S106-S115. [doi: 10.1016/j.pmrj.2017.02.018] [Medline: 28527495]
22. Kotz D, Gunter CA, Kumar S, Weiner JP. Privacy and security in mobile health: a research agenda. Computer (Long Beach Calif) 2016 Jun;49(6):22-30 [FREE Full text] [doi: 10.1109/MC.2016.185] [Medline: 28344359]
23. Krebs P, Duncan DT. Health app use among US mobile phone owners: a national survey. JMIR Mhealth Uhealth 2015 Nov 04;3(4):e101 [FREE Full text] [doi: 10.2196/mhealth.4924] [Medline: 26537656]
24. Wiesner M, Zowalla R, Suleder J, Westers M, Pobiruchin M. Technology adoption, motivational aspects, and privacy concerns of wearables in the German running community: field study. JMIR Mhealth Uhealth 2018 Dec 14;6(12):e201 [FREE Full text] [doi: 10.2196/mhealth.9623] [Medline: 30552085]

25. Di Matteo D, Fine A, Fotinos K, Rose J, Katzman M. Patient willingness to consent to mobile phone data collection for mental health apps: structured questionnaire. JMIR Ment Health 2018 Aug 29;5(3):e56 [FREE Full text] [doi: 10.2196/mental.9539] [Medline: 30158102]
26. Goldenberg T, McDougal SJ, Sullivan PS, Stekler JD, Stephenson R. Preferences for a mobile HIV prevention app for men who have sex with men. JMIR Mhealth Uhealth 2014 Oct 29;2(4):e47 [FREE Full text] [doi: 10.2196/mhealth.3745] [Medline: 25355249]
27. Goldenberg T, McDougal SJ, Sullivan PS, Stekler JD, Stephenson R. Building a mobile HIV prevention app for men who have sex with men: an iterative and community-driven process. JMIR Public Health Surveill 2015 Nov 16;1(2):e18 [FREE Full text] [doi: 10.2196/publichealth.4449] [Medline: 27227136]
28. Kenny R, Dooley B, Fitzgerald A. Developing mental health mobile apps: exploring adolescents' perspectives. Health Informatics J 2016 Jun;22(2):265-275 [FREE Full text] [doi: 10.1177/1460458214555041] [Medline: 25385165]
29. Proudfoot J, Parker G, Hadzi Pavlovic D, Manicavasagar V, Adler E, Whitton A. Community attitudes to the appropriation of mobile phones for monitoring and managing depression, anxiety, and stress. J Med Internet Res 2010 Dec 19;12(5):e64 [FREE Full text] [doi: 10.2196/jmir.1475] [Medline: 21169174]
30. Seh AH, Zarour M, Alenezi M, Sarkar AK, Agrawal A, Kumar R, et al. Healthcare data breaches: insights and implications. Healthcare (Basel) 2020 May 13;8(2):133 [FREE Full text] [doi: 10.3390/healthcare8020133] [Medline: 32414183]
31. Bondaronek P, Alkhaldi G, Slee A, Hamilton FL, Murray E. Quality of publicly available physical activity apps: review and content analysis. JMIR Mhealth Uhealth 2018 Mar 21;6(3):e53 [FREE Full text] [doi: 10.2196/mhealth.9069] [Medline: 29563080]
32. Müthing J, Jäschke T, Friedrich CM. Client-focused security assessment of mHealth apps and recommended practices to prevent or mitigate transport security issues. JMIR Mhealth Uhealth 2017 Oct 18;5(10):e147 [FREE Full text] [doi: 10.2196/mhealth.7791] [Medline: 29046271]
33. Papageorgiou A, Strigkos M, Politou E, Alepis E, Solanas A, Patsakis C. Security and privacy analysis of mobile health applications: the alarming state of practice. IEEE Access 2018 Jan 29;6:9390-9403. [doi: 10.1109/access.2018.2799522]
34. Klopfer PH, Rubenstein DI. The concept privacy and its biological basis. J Soc Issues 1977;33(3):52-65. [doi: 10.1111/j.1540-4560.1977.tb01882.x]
35. Posner RA. The economics of privacy. Am Econ Rev 1981 May;71(2):405-409.
36. Norberg PA, Horne DR, Horne DA. The privacy paradox: personal information disclosure intentions versus behaviors. J Consum Aff 2007 Mar 6;41(1):100-126. [doi: 10.1111/j.1745-6606.2006.00070.x]
37. Acquisti A. Privacy in electronic commerce and the economics of immediate gratification. In: Proceedings of the 5th ACM Conference on Electronic commerce. 2004 Presented at: EC '04; May 17-20, 2004; New York, NY, USA p. 21-29. [doi: 10.1145/988772.988777]
38. Hallam C, Zanella G. Online self-disclosure: the privacy paradox explained as a temporally discounted balance between concerns and rewards. Comput Human Behav 2017 Mar;68:217-227. [doi: 10.1016/j.chb.2016.11.033]
39. Hoffman LJ. Computers and privacy: a survey. ACM Comput Surv 1969 Jun;1(2):85-103. [doi: 10.1145/356546.356548]
40. Barth S, de Jong MD. The privacy paradox – investigating discrepancies between expressed privacy concerns and actual online behavior – a systematic literature review. Telemat Inform 2017 Nov;34(7):1038-1058. [doi: 10.1016/j.tele.2017.04.013]
41. Pavlou PA. State of the information privacy literature: where are we now and where should we go? MIS Q 2011 Dec;35(4):977-988. [doi: 10.2307/41409969]
42. Aïmeur E. Personalisation and privacy issues in the age of exposure. In: Proceedings of the 26th Conference on User Modeling, Adaptation and Personalization. 2018 Presented at: UMAP '18; July 8-11, 2018; Singapore, Singapore p. 373-376. [doi: 10.1145/3209219.3209271]
43. Varshney U. Mobile health: four emerging themes of research. Decis Support Syst 2014 Oct;66:20-35. [doi: 10.1016/j.dss.2014.06.001]
44. Xu H, Zhang C, Shi P, Song P. Exploring the role of overt vs. covert personalization strategy in privacy calculus. Acad Manag Proc 2009 Aug 15;2009(1):1-6. [doi: 10.5465/ambpp.2009.44249857]
45. Sutanto J, Palme E, Tan CH, Phang CW. Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users. MIS Q 2013 Dec;37(4):1141-1164. [doi: 10.25300/misq/2013/37.4.07]
46. Awad NF, Krishnan MS. The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. MIS Q 2006 Mar;30(1):13-28. [doi: 10.2307/25148715]
47. Gefen D, Straub DW. Gender differences in the perception and use of e-mail: an extension to the technology acceptance model. MIS Q 1997 Dec;21(4):389-400. [doi: 10.2307/249720]
48. MORRIS MG, VENKATESH V. Age differences in technology adoption decisions: implications for a changing work force. Pers Psychol 2000 Jun;53(2):375-403. [doi: 10.1111/j.1744-6570.2000.tb00206.x]
49. Morris MG, Venkatesh V, Ackerman PL. Gender and age differences in employee decisions about new technology: an extension to the theory of planned behavior. IEEE Trans Eng Manage 2005 Feb;52(1):69-84. [doi: 10.1109/tem.2004.839967]
50. Wang ES. Perceived control and gender difference on the relationship between trialability and intent to play new online games. Comput Human Behav 2014 Jan;30:315-320. [doi: 10.1016/j.chb.2013.09.016]

51. Venkatesh V, Thong JY, Xu X. Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. MIS Q 2012 Mar;36(1):157-178. [doi: 10.2307/41410412]
52. Featherman MS, Pavlou PA. Predicting e-services adoption: a perceived risk facets perspective. Int J Hum Comput Stud 2003 Oct;59(4):451-474. [doi: 10.1016/s1071-5819(03)00111-3]
53. Reuter T, Ziegelmann JP, Wiedemann AU, Lippke S, Schuz B, Aiken LS. Planning bridges the intention-behaviour gap: age makes a difference and strategy use explains why. Psychol Health 2010 Sep;25(7):873-887. [doi: 10.1080/08870440902939857] [Medline: 20204963]
54. Ziefle M, Röcker C. Acceptance of pervasive healthcare systems: a comparison of different implementation concepts. In: Proceedings of the 4th International Conference on Pervasive Computing Technologies for Healthcare. 2010 Presented at: PERVASIVEHEALTH '10; March 22-25, 2010; Munich, Germany p. 1-6. [doi: 10.4108/ICST.PERVASIVEHEALTH2010.8915]
55. Sintonen S, Immonen M. Telecare services for aging people: assessment of critical factors influencing the adoption intention. Comput Human Behav 2013 Jul;29(4):1307-1317. [doi: 10.1016/j.chb.2013.01.037]
56. Guo X, Sun Y, Wang N, Peng Z, Yan Z. The dark side of elderly acceptance of preventive mobile health services in China. Electron Mark 2012 Dec 11;23(1):49-61. [doi: 10.1007/s12525-012-0112-4]
57. Miles MB, Huberman M, Saldana J. Qualitative Data Analysis: A Methods Sourcebook. 3rd edition. Thousand Oaks, CA, USA: Sage Publications; 2014.
58. Flick U. An Introduction to Qualitative Research. 6th edition. Thousand Oaks, CA, USA: Sage Publications; Jan 2019.
59. Thomas DR. A general inductive approach for analyzing qualitative evaluation data. Am J Eval 2006 Jun 1;27(2):237-246. [doi: 10.1177/1098214005283748]
60. Swoboda W, Schmieder M, Bulitta C, Gaisser S, Hofmann GR, Kremer-Rücker P, et al. Die gemeinsame Ethik-Kommission der Hochschulen Bayerns – GEHBa. mdi - Forum der Medizin-Dokumentation und Medizin-Informatik 2021;3:80-83 [FREE Full text]
61. Xu H, Dinev T, Smith HF, Hart P. Examining the formation of individual's privacy concerns: toward an integrative view. In: Proceedings of the 2008 International Conference on Information Systems. 2008 Presented at: ICIS '08; December 14-17, 2008; Paris, France p. 6.
62. Baruh L, Secinti E, Cemalcilar Z. Online privacy concerns and privacy management: a meta-analytical review. J Commun 2017 Jan 17;67(1):26-53. [doi: 10.1111/jcom.12276]
63. Fruchter N, Liccardi I. Consumer attitudes towards privacy and security in home assistants. In: Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems. 2018 Presented at: CHI EA '18; April 21-26, 2018; Montreal, Canada p. 1-6. [doi: 10.1145/3170427.3188448]
64. Kennedy S, Li H, Wang C, Liu H, Wang B, Sun W. I can hear your Alexa: voice command fingerprinting on smart home speakers. In: Proceedings of the 2019 IEEE Conference on Communications and Network Security. 2019 Presented at: CNS '19; June 10-12, 2019; Washington, DC, USA p. 232-240. [doi: 10.1109/cns.2019.8802686]
65. Gross R, Acquisti A. Information revelation and privacy in online social networks. In: Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society. 2005 Presented at: WPES '05; November 7, 2005; Alexandria, VA, USA p. 71-80. [doi: 10.1145/1102199.1102214]
66. Kokolakis S. Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon. Comput Secur 2017 Jan;64:122-134. [doi: 10.1016/j.cose.2015.07.002]
67. Smith HJ, Dinev T, Xu H. Information privacy research: an interdisciplinary review. MIS Q 2011 Dec;35(4):989-1015. [doi: 10.2307/41409970]
68. Bansal G, Zahedi FM, Gefen D. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decis Support Syst 2010 May;49(2):138-150. [doi: 10.1016/j.dss.2010.01.010]
69. Bhattacherjee A, Premkumar G. Understanding changes in belief and attitude toward information technology usage: a theoretical model and longitudinal test. MIS Q 2004 Jun;28(2):229-254. [doi: 10.2307/25148634]
70. Sun H. A longitudinal study of herd behavior in the adoption and continued use of technology. MIS Q 2013 Dec;37(4):1013-1041. [doi: 10.25300/misq/2013/37.4.02]
71. Jiang R. Introducing new Alexa healthcare skills. Amazon Alexa. 2019 Apr 4. URL: https://developer.amazon.com/de/blogs/alexa/post/ff33dbc7-6cf5-4db8-b203-99144a251a21/introducing-new-alexa-healthcare-skills [accessed 2021-06-25]
72. Koppel R, Kuziemsky C. Healthcare data are remarkably vulnerable to hacking: connected healthcare delivery increases the risks. Stud Health Technol Inform 2019;257:218-222. [Medline: 30741199]
73. Lee DJ, Ahn JH, Bang Y. Managing consumer privacy concerns in personalization: a strategic analysis of privacy protection. MIS Q 2011 Jun;35(2):423-444. [doi: 10.2307/23044050]

Abbreviations

mHealth: mobile health
RQ: research question

Edited by G Eysenbach; submitted 17.02.21; peer-reviewed by E Baker, D Kotz, I Schiering; comments to author 24.03.21; revised version received 30.06.21; accepted 16.04.22; published 13.06.22

Please cite as:
Schroeder T, Haug M, Gewald H
Data Privacy Concerns Using mHealth Apps and Smart Speakers: Comparative Interview Study Among Mature Adults
JMIR Form Res 2022;6(6):e28025
URL: https://formative.jmir.org/2022/6/e28025
doi: 10.2196/28025
PMID: