To Disclose or Not to Disclose: Examining the Privacy Decision-Making Processes of Older vs. Younger Adults

Reza Ghaiumy Anaraky
rghaium@clemson.edu
Clemson University
Clemson, SC, USA

Kaileigh A. Byrne
kaileib@clemson.edu
Clemson University
Clemson, SC, USA

Pamela J. Wisniewski
pamwis@ucf.edu
University of Central Florida
Orlando, FL, USA

Xinru Page
xinru@cs.byu.edu
Brigham Young University
Provo, UT, USA

Bart P. Knijnenburg
bartk@clemson.edu
Clemson University
Clemson, SC, USA

ABSTRACT

To understand the underlying process of users' information disclosure decisions, scholars often use either the privacy calculus framework or refer to heuristic shortcuts. It is unclear whether the decision process varies by age. Therefore, using these common frameworks, we conducted a web-based experiment with 94 participants, who were younger (ages 19-22) or older (65+) adults, to understand how perceived app trust, sensitivity of the data, and benefits of disclosure influence users disclosure decisions. Younger adults were more likely to change their perception of data sensitivity based on trust, while older adults were more likely to disclose information based on perceived benefits of disclosure. These results suggest older adults made more rationally calculated decisions than younger adults, who made heuristic decisions based on app trust. Our findings negate the mainstream narrative that older adults are less privacy-conscious than younger adults; instead, older adults weigh the benefits and risks of information disclosure.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**; • **Human-centered computing → Empirical studies in accessibility**; *Empirical studies in HCI*.

KEYWORDS

Information privacy, older adults, young adults, affect heuristics, privacy calculus

ACM Reference Format:
Reza Ghaiumy Anaraky, Kaileigh A. Byrne, Pamela J. Wisniewski, Xinru Page, and Bart P. Knijnenburg. 2021. To Disclose or Not to Disclose: Examining the Privacy Decision-Making Processes of Older vs. Younger Adults. In *CHI Conference on Human Factors in Computing Systems (CHI '21), May 8–13, 2021, Yokohama, Japan.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3411764.3445204

CHI '21, May 8–13, 2021, Yokohama, Japan

ACM ISBN 978-1-4503-8096-6/21/05…$15.00
https://doi.org/10.1145/3411764.3445204

1 INTRODUCTION AND RELATED WORK

Older adults—individuals age 65 and above—make up 9% of the world's population [76] and their numbers are growing rapidly. By 2030, the older adult population is projected to reach 1 billion, which will be around 12% of the projected world population [83]. At 15%, the U.S. has an even higher percentage of older adults than the world average [78]. Despite the common perception of older adults as not using technology, a 2009 survey showed that around 40% of them use computers and the Internet [18], and a 2013 report showed that 42% of older adults have smartphones [7]. Internet and technology use are intertwined with privacy concerns for all populations [15, 79]. As 70% of online older adults use it on a daily basis [104], they constitute a major group of Internet users who have privacy concerns [17, 20, 21, 70].

1.1 Older Adults vs. Younger Adults and Privacy

Narratives around technology use and older adults tend to focus on older adults' deficits and difficulties keeping up with younger adults. For instance, Tacken et al. [89] found that many older adults show resistance in adapting to the rapid succession of new technologies [89], and Roger et al. [85] also found that it takes additional time for older adults to learn a new technology. Similarly, Czaja et al. [26] uncovered that technology use tends to lead to more anxiety and lower self-efficacy for older adults compared to younger adults. These deficit-based narratives extend into the domain of privacy research as well. Much of the privacy literature examining age-related differences in digital privacy has characterized older adults as having more difficulty than younger adults when managing their digital privacy (e.g., [10, 11, 55, 80, 93]) and generally less likely to protect themselves against privacy risks [90, 102]. For instance, Brandtzæg et al. [11] interviewed Facebook users about privacy features and found that younger adults have an easier time locating and understanding these features compared to older adults. Shujing and Tao's [88] survey-based study concluded that older adults demonstrate low privacy awareness, lack digital literacy, do not pay attention to privacy options, and thus are prone to disclosing too much information online. At the same time, older adults have also been shown to have higher levels of privacy concern than younger adults [81, 93]. Yet, Van den Broeck et al.[93] found that this heightened privacy concern does not translate to more privacy

protective actions; they divided participants aged 18 to 65 into three age groups and found that while the oldest group reported more privacy concerns, younger users used more privacy control features. To address these heightened privacy concerns, older adults sometimes avoid the use of digital technologies, such as social media [81]. One possible explanation for lower use of privacy features of older adults may be that they lack the digital literacy to use such features. Indeed, Park identified a digital divide in technology skills based on age, which was associated with older adults having less privacy control overall [80]. In contrast, Miltgen and Peyrat-Guillard found that younger adults express more positive attitudes around data management and are more confident in their ability to prevent data misuse than older adults [74]. Overall, such findings have led many scholars to conclude that older adults are more vulnerable to security and privacy threats than younger adults[10].

As demonstrated through the findings above, the literature tends to emphasize the deficits of older adults compared to younger adults when it comes to their privacy behaviors, adoption, and use of digital technologies. Yet, focusing on the technology skill deficits of older adults can have detrimental long-term effects by reducing older adults' overall interest and desire to engage with technology in a way that benefits them [73]. While older-adult-friendly designs may account for age-related changes in motor control, perceptual function, and cognitive ability, many technologies do not tailor their services to older adult populations [33, 36, 84]. Indeed, Frik et al.[36] urge designers and developers to specifically consider the older adult population when developing new products. They identify common misconceptions among older adults (e.g., if they have nothing to hide, they should not be worried about privacy) and argue that product designers should consider these beliefs in order to design effective systems that can empower older adults. Thus, the problems associated with older adults' technology use may instead be due to the deficits in the design of technologies, which often cater to the needs of younger adults.

Some scholars are moving away from painting older adults as technology Luddites. For example, Knowles and Hanson [55] took a strength-based approach by interviewing older adults to understand their resistance against technology adoption. They found that older adults had legitimate concerns regarding the use of digital technologies, and the risks associated with use often outweighed the benefits. As such, these researchers chose to emphasize the "wisdom" older adults demonstrated in their decision-making process not to engage with technology. Hoofnagle et al. [40] showed that younger and older adults are not different in terms of attention to privacy policies. They also asked participants some comprehensive questions to assess their online privacy knowledge. Overall, while only 12% of younger adults answered at least 3 out of 5 of the questions correctly, 25% of older adults performed that well. Indeed, older adults may not underestimate privacy risks [41], and their low technology use rate can be due to an informed privacy decision (i.e., non-use due to costs outweighing benefits) rather than an inability to learn [55]. Kropczynski et al. [59] show how older adults work as a community to approach their privacy issues.

However, the present research goes beyond these studies by focusing on the underlying decision-making processes that affect private information disclosures online and how these processes differ between these two age groups. Our intent is to not focus on the deficits of older adults when it comes to privacy, but instead, understand whether and how their privacy decision-making processes differ from younger adults.

1.2 Older Adults vs. Younger Adults and Decision-Making Processes

The psychological literature confirms that older and younger adults exhibit fundamental behavioral differences in their patterns of decision-making, including differences in risk preference and reliance on goal-driven strategies [97]. The relationship between aging and decision-making has been examined in several contexts. In risky choice contexts, older adults tend to be less risk-taking overall compared to younger adults [47]. However, older adults are often more willing to take risks to avoid a loss than obtain a gain compared to younger adults, although this relationship can vary depending on the magnitude of what is at stake [9, 14]. Furthermore, the age-related positivity effect also affects decision-making strategies. This effect refers to a tendency for older adults to have heightened attention or give more weight to positive information or stimuli during the decision-making process and less weight or attention to negative information [69]. Thus, if negative information is not completely salient in a given decision scenario, older adults may exhibit a bias to attend more to the positive aspects of a decision than negative aspects.

While this past research has highlighted age-related differences in privacy awareness, concerns, and protective behaviors, none of these studies have examined differences in the *privacy decision-making processes* of older and younger adults. Understanding how age is related to decision-making processes, rather than privacy attitudes and outcomes, can help us better understand the choices younger and older adults make regarding their privacy and the factors that must be considered when designing technologies to assist with their privacy decision-making.

1.3 Frameworks for Privacy Decision-Making and Disclosure

Many scholars have studied privacy decision-making using the privacy calculus framework [29, 30, 50, 58] which enables them to study users' disclosure decisions as a result of a trade-off between the rewards and the costs of disclosure [23, 61, 75]. Studies which use privacy calculus can understand the underlying reasons for privacy decisions in different contexts and can account for a reasonable amount of variation of the privacy decisions [50, 64]. For instance, Krasnova et al. [57] studied self-disclosure in the context of social media using the privacy calculus framework. To assess benefits, they measured the opportunities in social media for relationship maintenance, enjoyment, and self-presentation. To assess disclosure costs, they measured privacy concerns, perceived likelihood of various privacy violations, and perceived damage of a potential violation. Overall, they showed that a high perceived benefit and low perceived cost is positively associated with self-disclosure. Xu et al.[101] used a privacy calculus framework to study users' intention to disclose their location. Benefits of disclosure were measured as locatability (detecting the current physical location) and personalization (individualized functionalities which enhance the user experience). They also measured perceived risks based on users'

perceptions of loss associated with the release of personal information. They found that users who perceive a high benefit and a low risk are more likely to have a high disclosure intention. As demonstrated through these works, scholars have used a variety of different ways to operationalize the "costs" and "rewards" that are the antecedents of disclosure in the privacy calculus framework. The premise that perceived benefits and risks associated with disclosure are relevant trade-offs to consider when studying privacy decision-making outcomes has withstood the test of time.

The privacy calculus framework is, however, not without criticism. Some studies argue that users do not always weigh perceived costs against benefits in an entirely rational manner [3]. Privacy decisions are complex, and humans' ability to acquire and analyze all the relevant information is limited [2, 49]. Several researchers have demonstrated that users' privacy decisions are not always as deliberate as privacy calculus suggests, and that information disclosure can be easily influenced by spurious heuristic factors, such as default settings or the framing of the information request [3, 4, 6, 56]. Johnson et al. [46], for example, studied how framing and default settings influence users' privacy decisions. They found that if a privacy option is pre-selected by default or presented with a positive framing, users are more likely to accept it. John et al. [45] showed that environmental cues such as website design also influence disclosure decisions. Anaraky et al. [5] showed that Facebook users are more likely to accept a photo tagging request if the request is accompanied with any type of justification, even a justification against tagging. Dinev et al. [30] studied Internet users' willingness to provide personal information to complete transactions on the Internet. They found that while perceived privacy risks and privacy concerns inhibit disclosure (the costs of privacy calculus), trust of the Internet and personal interests can outweigh these costs and contribute to users' data disclosure decisions. These examples demonstrate that users' privacy decisions often rely on imprecise and heuristic processes that may seem paradoxical or irrational when studying users' privacy disclosure decisions [1, 8].

While the premises of privacy calculus—that users make a deliberate trade-off between the costs and benefits—might not totally hold true, privacy calculus is still a useful framework for analyzing users' privacy decision-making processes [53], but should be integrated to include the more nuanced and heuristic decision-making processes users employ when making privacy decisions. Therefore, researchers have introduced heuristic-based frameworks to better explain self-disclosure behaviors [95]. To leverage the merits of privacy-calculus and better account for heuristics, Wang et al. [95] integrated the privacy calculus framework with heuristic shortcuts. They found that, while the privacy calculus decision-making process generally held, peripheral cues and information asymmetry acted as heuristic factors that influenced users' disclosure decisions. Drawing from the findings of Dinev et al. [30] and Wang et al. [95], we augment the privacy calculus framework by examining app trust as a potential heuristic shortcut that users consider when disclosing personal information online. We test this integrated model to understand the effects of privacy calculus (i.e., benefits and costs) and heuristic short cuts (i.e., app trust) on users' information disclosure behavior. Further, we examine whether and how these effects are moderated by age group (i.e., older versus younger adults).

Contribution—Past literature has demonstrated differences between older and younger adults in terms of several privacy-related constructs (e.g., privacy awareness, use of privacy controls). However, our study is one of the first to investigate differences in the *mechanisms* by which older and younger adults make privacy decisions—the decision process that leads them to either disclose their data or withhold it from disclosure. As such, our contribution to the literature is to study age differences in the privacy decision-making *process* rather than merely focusing on the decision *outcomes*. To this end, we address the following high-level research questions:

> **RQ1:** *Do older adults disclose more personal information online than younger adults?*
>
> **RQ2:** *Do older adults differ from young adults in terms of how they make decisions to disclose personal information online?*

To answer these research questions, we recruited 94 participants to take part in a web-based user study. We recruited participants based on two different age groups—younger adults (ages 18-22) and older adults (65+)—to compare differences between these two groups. First, we presented a fictitious financial planning app (i.e., "CreditPush") to our participants. We described CreditPush as a financial app, which generates recommendations to help users improve their credit score and financial situation. Second, we asked participants to disclose various types of personal information (e.g., bank account balances, annual income, credit score) to use the app. We then asked participants to self-report on privacy-related constructs, including perceived app trust, sensitivity of the data, and benefits of disclosure. We analyzed our data by integrating two opposing privacy decision-making frameworks (i.e., privacy calculus [29, 30, 50, 58] and heuristic decision-making [3, 95]) into a cohesive theoretical model to understand how these constructs influenced participants' disclosure decisions. We then did a more in-depth analysis on this model based on age group to understand differences between younger adults and older adults in terms of their unique decision-making processes. To test our model, we conducted path analyses to examine the direct effects of our model constructs on the decision to disclose personal information to the app, as well as the moderating effects of age on this decision-making process.

Overall, sensitivity of the data was significantly and negatively associated with disclosure regardless of age group. App trust was negatively associated with sensitivity of the data and positively associated with benefits of disclosure. We found that older adults did not disclose a significantly different amount of information to the app compared to younger adults (RQ1), but significant differences emerged between younger and older adults in the *decision-making process* underlying their disclosure decisions (RQ2). Particularly, we found that:

- Older adults were less likely than younger adults to allow their trust in the app to influence their opinion of the sensitivity of data being shared.
- Older adults were more likely than younger adults to disclose information when they perceived greater benefits of disclosure.

Our results suggest that older adults demonstrate a more rationally-driven privacy calculus of weighing the benefits versus the risks of disclosure, while younger adults rely more heavily on heuristic decision-making driven by app trust. The overall contribution of this study is to illustrate the sources of age-related differences and translate them into design implications that foster correspondence between users' privacy decision-making processes and the characteristics of the technology.

2 RESEARCH FRAMEWORK

In the sections below, we introduce our research framework, which integrates the theory of privacy calculus (i.e., benefits and costs) with more heuristic processes (i.e., app trust) to understand users' information disclosure decisions.

2.1 Dependent Variable: Information Disclosure

Information disclosure is a commonly studied outcome variable within privacy research [30, 68, 100, 101] as users' privacy decisions typically involve choosing to withhold or disclose one or more types of personal information. Examples of information disclosure behaviors studied in past privacy research have ranged from whether to share one's financial information to complete an e-commerce transaction [29, 30], one's health data to benefit from a health-app [42] or online health communities [103], one's location to leverage location-based services [100], or one's personal information to use social networking sites [58].

Disclosing personal information may be advantageous for users, as it gives them access to better or more personalized services that leverage this data [100]. For example, while users might be able to browse an e-map in private mode, they must disclose their location to be able to use GPS features. Likewise, in a messaging app users can manually enter the recipient's email or phone number, but giving the app access to the user's contacts enables them to select an existing entry, thereby avoiding the hassle of having to type it themselves. The rewards of disclosure, however, come at the cost of diminished privacy: users may worry that their safety could be compromised if their location data is hacked, or they might fear that the messaging app might use their contact list for promotional activities. Users thus have to decide whether to disclose their information and obtain some gratification or to withhold from disclosure and maintain their privacy. In our study, we treat the decision to disclosure personal information to a fictitious financial planning app as our outcome variable of interest.

2.2 Privacy Calculus: Perceived Benefits vs. Costs of Disclosure

As outlined in Section 1.3, privacy calculus is a well-studied framework for studying the trade-off between the benefits and costs of the disclosure [61]. However, studies have used different approaches to operationalize these antecedents. In our study, we examined the benefits of disclosure by first asking participants to disclose or withhold several pieces of information to a fictitious financial app. Each of these disclosure decisions involves a trade-off between the rewards and the costs of disclosure. To assess the benefits of disclosure, we asked participants to rate how much they felt the information requested would improve the *quality of recommendations* provided by the app. There is a large body of literature exploring the trade-offs between privacy and personalization [99]. In our case, the quality of the recommendation served as a form of personalization [100], thus a potential benefit of disclosure when using a financial planning app.

To assess costs associated with disclosure, we measured *perceived data sensitivity*. Perceived data sensitivity has been associated with heightened disclosure risks [64], privacy concerns [98], and fewer information disclosures [68] in past literature. Based on the privacy calculus framework and the aforementioned operationalizations of costs and benefits, we pose the following hypotheses:

H1: *Perceived quality of recommendation will be positively associated with information disclosure.*

H2: *Perceived sensitivity of data will be negatively associated with information disclosure.*

2.3 App Trust as a Heuristic for Disclosure

A heuristic is a strategic or mental shortcut that often involves considering some information and discarding others when making a decision [43]. Some scholars study trust as a heuristic [62, 96, 105]. Lewicki et al. [62], for example, present trust as an "affect heuristic" that shapes judgements especially for some decision makers who rely on this heuristic and ignore other information when making a decision. Therefore, a heuristic view of trust suggests that high trust may streamline the disclosure decision making process [86]. While most studies in the field do not conceptualize trust as a heuristic, trust has been commonly used as an antecedent in studies that use the privacy calculus framework [16, 24]. Xu et al. [100], for example, showed that users who have more trust in a service provider also have lower perceived levels of privacy risks and are more willing to disclose information to that service provider. Gong et al. [38] studied people's attitudes towards online health services. They not only showed that users with high trust have lower risk perceptions, but they also found that highly trusting users perceive higher levels of benefit. We use a 4-item construct to measure a user's trust in the app adopted from previous literature [44, 52, 71]. In line with past findings, we pose the following hypotheses:

H3: *App trust will be positively associated with information disclosure.*

H4: *App trust will be positively associated with perceived quality of recommendation.*

H5: *App trust will be negatively associated with perceived data sensitivity.*

2.4 Older Adults vs. Younger Adults and Disclosure

A person's age may have two distinctive effects on privacy decisions: it can be associated with higher or lower levels of disclosure (i.e., a main effect on disclosure), or it can influence the *process* by which information disclosure will come about (i.e., a moderation of the effects in the privacy calculus framework). The former effect has been investigated in considerable detail with privacy literature. In terms of the main effect of age on disclosure, the existing evidence is mixed. Jourard [48] did not find any significant overall relationships between age and self-disclosure. Little et al. [66], on

the other hand, found an overall U-shaped trend in disclosure levels in which younger (under 35) and older (above 56) individuals disclose the same amounts of information while individuals from 35 to 55 disclose less information compared to younger and older groups. Meanwhile, other studies have shown that older adults take fewer privacy protective actions, which lead to more online information disclosures [88]. Given these mixed findings, we chose to hypothesize that older adults disclose more personal information online, which makes them more vulnerable to privacy threats. While we do not necessarily ascribe to this deficit-based narrative, it is an uncommon practice to test a null hypothesis of no differences, and our primary intention is to investigate whether this deficit-based assumption about older adults holds true. Therefore, H6 corresponds to our RQ1:

H6: *Older adults will disclose significantly more information online than younger adults.*

Meanwhile, understanding the effect of age on the process by which information disclosure occurs is a novel contribution of this work. While there are several studies in the information privacy literature highlighting privacy deficits around how older adults manage their digital privacy, these studies often build on the premise that older adults are not as technologically skilled or as privacy-aware as their younger counterparts, and therefore, are more prone to privacy threats. These studies focus on the relative *value* of the antecedents of disclosure (e.g., whether older adults have lower privacy awareness [88]), while we explicitly study differences in the *impact* of these antecedents on participants' privacy decisions (e.g., whether privacy awareness has a different impact on decisions for older than younger adults)—the existence of such differences would indicate that older adults' decision mechanisms are different from those of younger adults. Our work is one of the first to examine the moderating effects of age on the privacy calculus and heuristic decision-making processes of younger versus older adults.

Figure 1 summarizes the hypothesized relationships between users' perceptions of app trust, sensitivity of the data, quality of the recommendation, and disclosure in our model (H1-H5; see Sections 2–2.3). We also test the assumption that older adults disclose more information online than younger adults (H6/RQ1). However, a key contribution of this work is that we go beyond these direct effects and examine the moderating effects of age group (i.e., older vs. younger adults) on the privacy decision-making processes associated with our model constructs (RQ2). Due to the novel and exploratory nature of this analysis, we chose not to explicitly pose hypotheses for the moderating effects of age group; rather, we report the relationships that were found in our results.

3 METHODS

3.1 Study Overview

To address our research questions and test our hypothesized model, we designed an online study. One of our objectives in this study was to overcome the shortcomings of studies with hypothetical scenarios and obtain ecological validity. Therefore, we developed a realistic yet fictitious web application called CreditPush: a financial app which purportedly could provide its users with tips to increase their credit score. After reading the consent form and agreeing to participate in the study, participants were redirected to the app. The first page of the app had some general information about its purpose. In the second and the third page, participants were asked several personal data-items (See Table A1 for a list of data-items) and could choose to disclose or not to disclose their data. We provide screenshots of the app in Figure A1. After interacting with the app, participants were redirected to a survey where we measured the constructs described in our research framework (see Figure 2).

3.2 Operationalization of Constructs

3.2.1 Dependent Variable: Information Disclosure. Participants were given the opportunity to disclose 12 personal information items to the app (see Table A1 for a full list of these items). Each of these 12 items were relevant to the context of the app and were chosen after a discussion session with several graduate students. Participants were told that disclosure was not required, but disclosing any of this information could increase the recommendation quality offered by the app. Participants were also instructed that if they were unsure of the exact value of a questionnaire item and they wanted to disclose it, then they could give their best estimates. Prior to the experiment, we had made it clear that participants' incentives were not contingent upon their responses. In addition, participants did not have an incentive to provide false or misleading information, because such information could adversely influence the app-generated recommendations and make the recommendations misleading or inaccurate. In cases that participants were not willing to disclose their data, they could select a "prefer not to disclose" option. However, to make sure participants did not consider themselves anonymous, disclosing their email address to the app was mandatory. Non-anonymity was important because there are minimal risks associated with disclosing non-identifiable data while being anonymous. We used participants' decision to disclose (or withhold) as the dependent variable. Unlike the majority of past studies, which measure overall *intention to disclose* data with multiple-scale items, we measured actual disclosure decisions of the data items as binary variables (coded as 1 for disclosure and 0 for non-disclosure).

3.2.2 Independent Variables. Participants were informed that their data would be used to improve app-generated personalized financial advice, and subsequently we measured the extent to which participants believe disclosing each of the items could improve the app-generated recommendations on a 1 (Strongly Disagree) to 7 (Strongly Agree) Likert scale [54]. We also used participants' subjective perceptions of data sensitivity as a proxy for costs of disclosure. Participants were asked about the perceived sensitivity levels of each of the 12 data items on a 4-point Likert scale (Not at all sensitive to very sensitive) [68]. Similar to how we measured disclosure, we also measured the perceived benefits (i.e., quality of recommendation) and costs (i.e., data sensitivity) associated with disclosing each data item individually.

App trust was another independent variable of our study; since trust is an attribute of the app rather than individual data items, measuring it on an item-basis is not applicable. We therefore measured trust of the app using a 4-item construct (e.g. "I believe CreditPush is honest when it comes to using the information I provide"–see Table A2 to check other items) which was validated in several previous works [44, 52, 71]. Figure 2 shows our experimental setup.

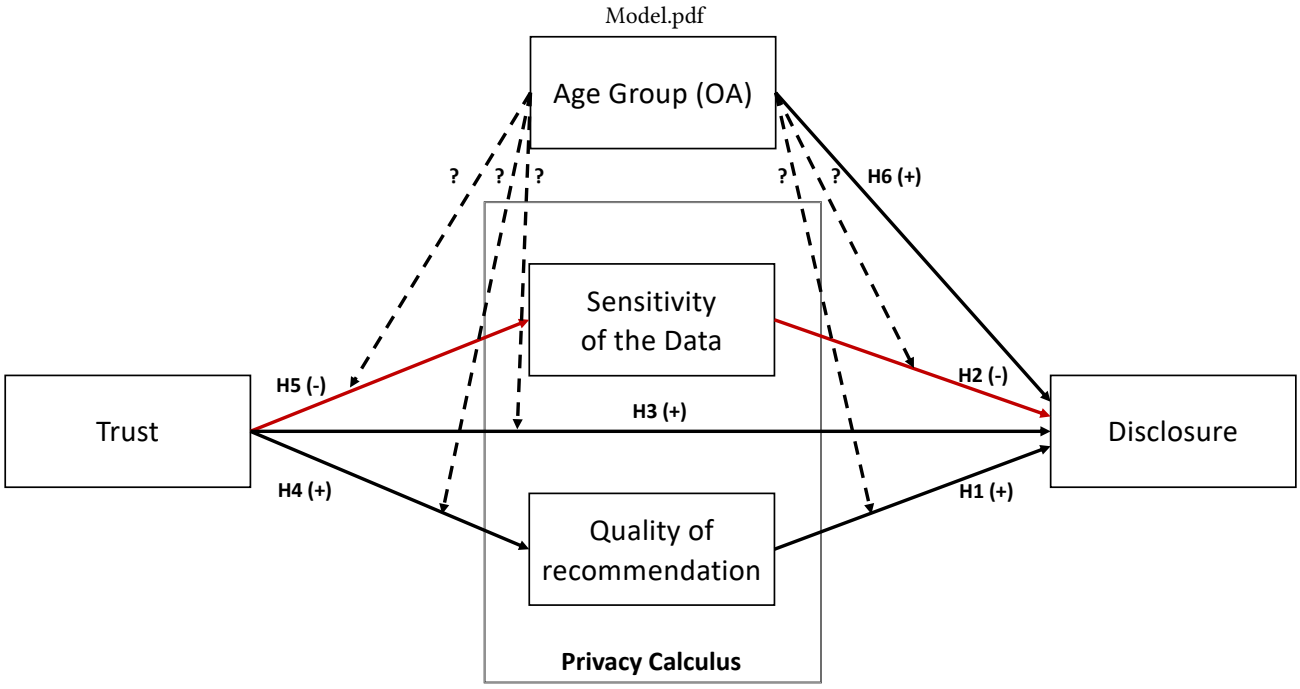


Figure 1: The hypothesized model and research questions

Interaction with the app

Questions about sensitivity, relevance, and trust

Figure 2: The experimental setup. After interacting with the app, participants were directed to a survey.

3.3 Participant Recruitment

The study sample consisted of older and younger adults. The U.S. Census Bureau and Centers for Disease Control (CDC) define older adults as individuals with the age equal to or above 65 years old and younger adults as individuals aging between 18 and 34 years old [13, 51]. Following these guidelines, we recruited participants within that age range. We initially recruited 117 participants; however, twenty-three participants failed to correctly answer the attention check questions and were excluded from the analysis. Therefore, our sample consisted of 94 participants, including 34 older adults (ages 65 - 86, M=73.59 years, SD=4.28 years), and 60 younger adults (ages 18 - 22, M=19.22 years, SD=1.15 years; see Table 1). The younger adults were recruited through a university recruitment system and received extra credit for their participation. The older adults were recruited through email communication and fliers at local community centers, educational locations (i.e., local Osher Lifelong Learning Institutes, college campuses), and retirement communities throughout the Greenville-Anderson-Mauldin, SC metropolitan area. Older adults received a $30 gift card for participating. The older adults sample also passed the Montreal Cognitive Assessment (MoCA) test which is used for accurately screening mild cognitive impairment, dementia, and normal aging [34, 60]. Research shows that the MoCA test is superior in overall sensitivity for detecting these different cognitive states than other similar tests such as Mini Mental State Exam (MMSE) [82]. Consequently, none of our older adult participants were diagnosed with a neurological illness, such as Alzheimer's disease or stroke. Furthermore, all of our older and younger adult participants had used computer and internet before and therefore were familiar with such technologies. This

is important since older adults represent a more heterogeneous population compared to younger adults because their educations, experiences, and health and living conditions are more variable [39, 65]. Lastly, this study was reviewed by an institutional review board and informed consent was obtained from all the participants prior to their participation. Participants were debriefed about the purpose of the study after their participation.

3.4 Data Analysis Approach

During the study, participants made 12 disclosure decisions of financial information relevant to improving the quality of the CreditPush app recommendations. We considered this behavior (whether to disclose or to withhold) as a binary dependent variable. Two of our independent variables were the elements of privacy calculus: participant's subjective perceived sensitivity of each data and their perceived improvement of recommendation quality by disclosing that data. These two variables were repeatedly measured based on the 12 data points of disclosure asked by the app. We also measured the extent participants trust the app with a 4-item pre-validated construct. We used Cronbach's Alpha to re-confirm trust's internal consistency. Cronbach's Alpha being above 0.7 (α = 0.973) suggests a good internal consistency for the trust construct [22]. Therefore, we calculated its sum-score and used it in our model. We standardized trust, perceived sensitivity, and perceived recommendation improvement variables for analysis. We also centered age group variable where OAs with the age of 65 and above were dummy coded as 0.5 and YAs were dummy coded as -0.5. To analyze our data, we conducted a multilevel logistic regression model with a random intercept to account for repeated measurements per participant. We first ran a saturated model [63], which included all paths for two and three-way interaction effects. Then, we trimmed paths that were not significant. Lastly, among our participants, there were 72 females and 22 male participants. Since our sample was not gender-balanced we controlled for participants' gender.

4 RESULTS

Our model's fit indices suggest a good fit. Although the chi-square test shows a significant misfit of $\chi^2(12) = 24.696, p = 0.016$, having a significant chi-square value is not unexpected in analyses with a relatively large number of records. Scholars used other metrics such as dividing the chi-square value by the degrees of freedom [51, 91]. That value is below 3, which is an indication of a good fit (2.058 in our case). Furthermore, the RMSEA of our model has a 90% confidence interval length of 0.035 and is below the cutoff threshold of 0.05 (RMSEA = 0.031) which is another indicator of a good fit [19].

4.1 The Main Effects of Privacy Calculus: Benefits and Costs of Disclosure

We hypothesized that the perceived improvement of the quality of the recommendations (i.e., disclosure benefits) would be positively associated with participants' information disclosure decisions (H1). However, this hypothesis was not supported. With each one standard deviation increase in perceived benefits, participants were a mere 2.1% more likely to disclose the information, which was not statistically significant ($p = .791$). Yet, there was a significant interaction effect of age group, which is reported in section 4.3. For H2, we found a significant, negative effect of data sensitivity on disclosure. With each one standard deviation increase in data sensitivity, participants were 27.1% less likely to disclose their information to the app ($p < .0001$). Thus, H2 was supported.

Table 1: Our sample characteristics.

	Older Adults	Younger Adults
N	34	60
Gender		
– Female	19	52
– Male	15	8
Age		
– Mean	73.588	19.216
– SD	4.279	1.151

4.2 The Main Effects of App Trust

H3 hypothesized that app trust was significantly and positively associated with information disclosure. However, this hypothesis was not supported. While with each one standard deviation increase in app trust the odds of disclosure were 17.1% higher, this effect was not significant ($p = .0.107$).

H4 and H5 were supported, though: App trust was positively associated with the perceived improvement in quality of the recommendation and negatively associated with the perceived sensitivity of the data. We found that with each one standard deviation increase in app trust, participants perceptions of data sensitivity decreased by 0.203 standard deviations ($p < .001$) and their perceived improvement in quality of the recommendation increased by 0.282 standard deviations ($p < .001$).

4.3 The Effects of Age Group

Next, we tested H6, which hypothesized that older adults would disclose significantly more information to the app than younger adults. We did not find significant differences between younger and older adults in terms of amount of disclosure ($p = .0.438$). Thus, H6 was rejected.

Then, we examined the non-hypothesized relationships in our model with respect to age group. First, we uncovered a significant positive main effect of age group on the perceived sensitivity of the data: Older adults perceived their data 0.193 standard deviations more sensitive ($p = .005$) than younger adults.

We also found two significant moderating effects of age group. First, age group moderated the relationship between perceived improvement of the quality of the recommendations (i.e., disclosure benefits) and disclosure. Figure 4a graphs this effect. For older adults, there was a positive correlation between the perceived improvement to the quality of the recommendations, while for younger adults, this relationship trended in the opposite direction. With each one standard deviation increase in perceived disclosure benefits, older adults were 20.9% more likely to disclose their data ($p = .031$) compared to younger adults.

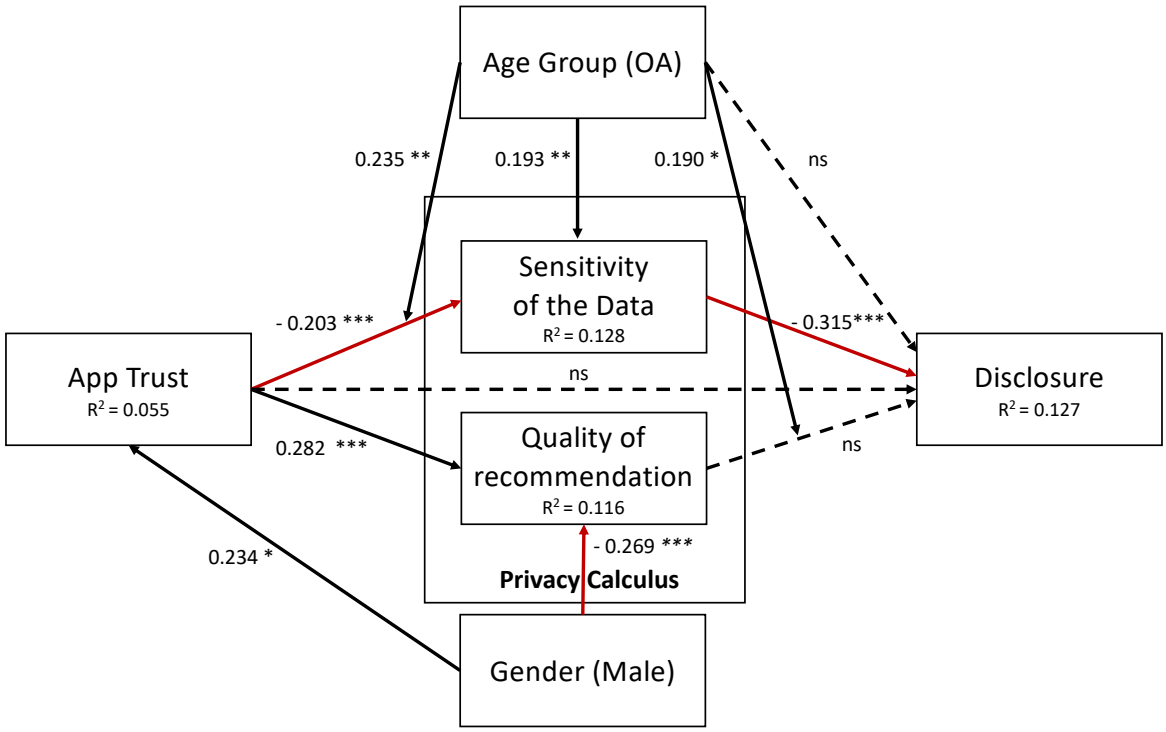
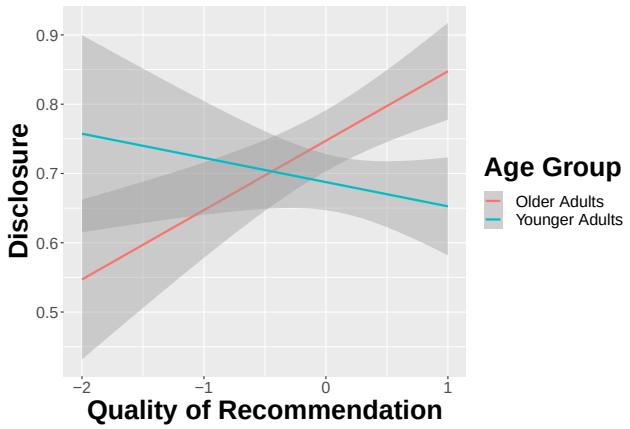
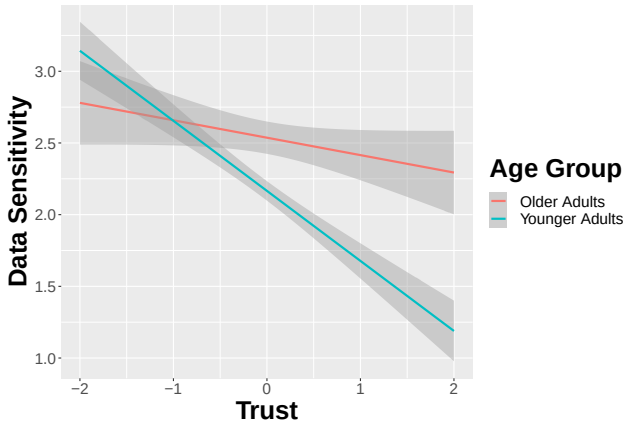


Figure 3: The path model including all of the significant findings (ns: not significant, * p < .05, ** p < .01, *** p < .001)



(a) Compared to younger adults, older adults are more likely to disclose data if they find it beneficial.



(b) Younger Adults who trust the app more also perceive their data being less sensitive. On the other hand, trust doesn't influence older adults' perceived data sensitivity.

Figure 4: Age group moderates the effect of benefits of disclosure on disclosure (a) and trust on perceived data sensitivity (b).

In addition, we found that age group moderates the effect of trust on perceived data sensitivity ($p = .001$). Since the main effects of age group and trust on data sensitivity are also significant, all these effects should be studied together. Figure 4b shows that while older adults data sensitivity is not a function of trust, younger adults heavily rely on trust such that if they trust the app more they perceive their data being less sensitive.

The negative effect of data sensitivity on disclosure was stronger for older adults than younger adults; with each one standard deviation increase in perceived data sensitivity, older adults were 9% less likely to disclose their data than younger adults. However, this effect did not reach significance ($p = .219$). Lastly, the effect of trust on perceived improvement in recommendation quality and on

Table 2: A summary of our findings. Odds Ratios (OR) are calculated for the disclosure decisions where the outcome variable is binomial

Variables	*b* (OR)	SE	*p*	Hypothesis Tests
DV: Disclosure				
Recommendation Quality (H1)	0.021 (1.021)	0.079	0.791	Not Supported
Data Sensitivity (H2)	**-0.315 (0.729)**	**0.076**	**<0.0001** ***	**Supported**
Trust (H3)	0.158 (1.171)	0.098	0.107	Not Supported
Age Group (Older vs. Younger Adults — H6)	0.086 (1.089)	0.110	0.438	Not Supported
Age Group X Recommendation Quality	**0.190 (1.209)**	**0.088**	**0.031** *	-
Age Group X Sensitivity	-0.095 (0.909)	0.078	0.219	-
Age Group X Trust	-0.048 (0.953)	0.127	0.708	-
Gender (Male vs. Female)	0.048 (1.049)	0.118	0.686	-
DV: Recommendation Quality				
Age Group (Older vs. Younger Adults)	0.022	0.181	0.902	-
Trust (H4)	**0.282**	**0.055**	**<0.0001** ***	**Supported**
Age Group X Trust	-0.157	0.168	0.350	-
Gender (Male vs. Female)	**-0.269**	**0.067**	**<0.0001** ***	-
DV: Data Sensitivity				
Age Group (Older vs. Younger Adults)	**0.193**	**0.068**	**0.005** **	-
Trust (H5)	**-0.203**	**0.058**	**<0.0001** ***	**Supported**
Age Group X Trust	**0.235**	**0.069**	**0.001** **	-
Gender (Male vs. Female)	-0.087	0.065	0.181	-
DV: Trust				
Age Group	0.038	0.111	0.345	-
Gender (Male vs. Female)	**0.234**	**0.110**	**0.033** *	-

disclosure were also not significantly moderated by the age group ($p = .350$, $p = .708$).

Figure 3 shows the significant direct and moderating effects of age group. All paths not drawn in this model were non-significant. The only non-significant paths (shown with dashed lines) drawn in this model are relationships that were hypothesized in our research framework. Statistically significant negative associations are drawn in red. Table 2 summarizes our findings.

4.4 The Effects of Gender

While controlling for gender, we found some significant effects. Males trusted the app more by 0.234 standard deviations than females ($p = .034$). Overall, males also perceived disclosure 0.269 standard deviations less beneficial than females ($p < .001$).

5 DISCUSSION

5.1 Calculus-based vs. Heuristic Privacy Decision-Making Processes

Our results show that users employ a hybrid process that integrates heuristics, such as taking into account the perceived trust in the app, along with making calculated assessments of the benefits and costs of disclosure. One important implication of our findings is that such heuristics did not overshadow the deliberation of privacy calculus, as we did not see a significant main effect of app trust on disclosure. Instead, heuristics of assessing app trust were antecedents that factored into the process of weighing the trade-offs associated with disclosure, as opposed to directly informing one's disclosure decisions. As such, our model demonstrates why it is imperative to take into account a hybrid decision-making approach—privacy calculus integrated with heuristic considerations—when studying privacy disclosures. Neither approach alone would sufficiently capture the decision-making process of all our participants; the true effects would be obscured or diluted if we only drew on privacy calculus, or only on heuristic-based privacy decision-making models.

Privacy calculus assumes that people make calculated decisions [23, 61]. Contrary to this traditional view, research on privacy decision making suggests that decisions are also driven by heuristics [4]. Therefore, scholars developed frameworks to square the privacy calculus and heuristic viewpoints and found that both these viewpoints can work together and complement each other in terms of understanding users' privacy decisions [94]. Likewise, our results show that both viewpoints are accurate when considered together. It follows that focusing on an exclusive rational or heuristic view cannot fully explain the underlying mechanism of privacy decision making.

People make calculated privacy decisions, but they also use heuristics to help them with this process due to imperfect or incomplete information. We suggest future research to consider taking this hybrid approach and explore not only the main effects of privacy calculus and heuristics on disclosure, but interaction effects of theoretically meaningful user characteristics, such as age or culture. For example, disclosure of information to different audiences could trigger different privacy decision-making processes. Transactional relationships (e.g., merchant) might elicit more privacy calculus type evaluations, while intimate trust-based relationships (e.g., partner) might evoke more of a heuristic approach.

5.2 The Privacy Calculus of Older Adults

In this paper, our goal was to study the extent to which older adults differ from young adults in terms of how they make decisions to disclose personal information. By doing this, we employ a strength-based approach of examining the positive characteristics of older adults and their privacy decision-making processes. Contrary to the deficit-based narrative in the literature for older adults, when it comes to managing their digital privacy, we found that older adults made informed privacy decisions based on the benefits and costs associated with disclosure. The privacy calculus process was actually more pronounced for older adults compared to younger adults, such that their disclosure decisions were not only based on data sensitivity, but also on anticipated benefits of disclosure.

This finding is in line with the psychological literature that suggests that older adults are more likely to think about long-term outcomes and be goal driven compared to younger adults [27, 72, 97]. Worthy et al. [97] suggests that older adults have a model-based way of thinking and are more goal-driven than younger adults. In a model-based system, individuals create a cognitive model of the environment. They are concerned with the way different states of the world are connected to each other [27, 31], think about long-term outcomes [27], and are goal-driven [72]. Gläscher et al.[37] compare the model-based system with the game of chess in which the player seeks future states (or moves) and evaluates the *rewards* associated with them. Although model-based decision making is more computational demanding and effortful, it is also more flexible and can be easier adjusted to the environment [32]. On the other hand, in a model-free system subjects do not simulate a cognitive model of the environment; past experiences and outcomes in one's environment are relied upon less, and heuristics are more likely to govern decisions. Therefore, predictions of future reward outcomes are less pronounced. This model-free way of thinking seemed to be more characteristic of younger adults, which we will discuss next.

5.3 The Heuristic of Trust for Younger Adults

The two significant moderating effects of age group shown in Figure 4a and 4b paint an interesting picture for younger adults. First, younger adults did not seem to weigh the perceived benefits of disclosure (i.e., improved quality of recommendations) in their decision to disclose information to the app. In fact, the trend in Figure 4a for younger adults was negative, which from a privacy calculus perspective would appear counter-intuitive. This finding suggests that younger adults may not value sharing more information for the purpose of personalizing financial recommendations to improve their credit score. A potential explanation for this outcome may be that younger adults have a relatively low financial literacy and are less attuned to their finances than older adults, as they are just starting to build their credit history [12, 28]. Therefore, impersonal recommendations may have seemed as useful to these participants as ones that were personalized to their financial situations.

In Figure 4b, we also see how younger adults rely heavily on the heuristic of app trust when evaluating the perceived sensitivity of the data being shared with the app.

From a heuristic perspective, it is plausible to argue that trusting the app will make younger adults feel safer and perceive less threat. Research shows that trust can function as a cognitive heuristic and guide individuals' risk perceptions [25, 62]. This seems to be the case here for younger adults who derive their sensitivity perceptions based on affect heuristic of trust. Emotions and heuristics act as mental shortcuts, whereby people access their pool of positive and negative feelings toward an issue to guide judgement [92]. On the other hand, older adults seem to consider data sensitivity as an inherent aspect of each data-item, and the level of trust does not significantly influence older adults' perceptions of data sensitivity. Furthermore, the risk-as-feeling hypothesis [67] suggests that emotional reactions to situations involving risk often block cognitive assessments of the situation and therefore heuristics drive such behavior. In our scenario, data sensitivity, which is significantly influenced by heuristics, was the only predictor for younger adults' disclosure decisions. In line with Worthy et al. 's [97] findings, our results suggest that younger adults' decisions are more driven by heuristics than older adults.

Furthermore, when taking into account that privacy is contextual, Nissenbaum's framework of contextual integrity [77] asserts that the recipient of the information (in this case, the CreditPush app) should be as important of a factor in assessing the appropriateness of information flows. Therefore, contextual integrity might also partially explain the heuristic decision-making process of younger adults. Similar to Miltgen and Peyrat-Guillard [74], who uncovered a "reversed" privacy paradox where younger adults expressed fewer privacy concerns but greater protective behaviors than older adults, we uncovered some interesting patterns among younger adults that seemed counter-intuitive to the privacy calculus framework but aligned with more heuristic decision-making processes. Therefore, we suggest additional research be conducted to further explore and unpack these relationships.

5.4 Implications for Design

A goal in privacy research is to help users make well-informed decisions. Some older adults believe that they are left out of the design process and not being attended to [35]. Our results suggest that it is important to show older adults the value or benefits of sharing information online. If disclosure gratifications are not clearly identified, companies cannot simply rely on established relationships with older adults for them to be willing to share information. Traditional trust indicators like brand name may not be enough to reassure these users that disclosure is in their best interests. Efforts to design an app or website with outward signs of, e.g., reliability and trustworthiness may not be as effective as providing information on how and why disclosing will be beneficial. Nonetheless, for young adults, it may be vital to establish a trusting relationship that can make users feel more comfortable disclosing information.

This finding suggests that researchers need to focus more on uncovering the perceived benefits and risks of disclosure for older adults. For example, findings that older adults use privacy features less, or are less privacy aware, might shift their focus to the costs associated with becoming familiar with privacy features or aware of privacy threats. These costs can be balanced against older adults' perceived benefit to better understand their disclosure decisions. This shift in emphasis could also shift the solution focus to ways of lowering these costs.

While using heuristics can greatly simplify disclosure decisions, this can also put young adults at risk of making disclosure decisions against their best interests. Products need to be aware that the disclosure decisions of their young adult users may not actually reflect their true feelings about the sensitivity of the information. Just because they share a piece of information does not necessarily give the green light for fully exploiting the data. An important area of research is to investigate designing opportunities for deliberate reflection on benefits and risks of disclosing data. This can help us understand how to help young adults avoid the pitfalls of mismatch between benefits of disclosing and overly trusting an app or website.

These design implications also emphasize how the product design can be a force for good, helping people focus on the benefits and drawbacks of disclosing their information, or could completely obscure these trade-offs. We call on product developers and designers to be cognizant of the heuristics that users may rely on by default, and to design in a way that will serve the users' best interests. With the increasing reach of technologies in every life domain, whether financial, social, political, or personal, designers and developers need to be aware that their product will somehow influence users, and they need to be explicit in the design and development of their products to avoid side effects that could unwittingly harm their users, and even society at large.

6 LIMITATIONS AND FUTURE WORK

Prior to concluding, we would like to highlight some of the limitations of our research and areas for future research. First, older adults are a heterogeneous group with different technical skills, physical, and cognitive conditions [39, 65] and we only recruited participants who passed cognitive tests, were familiar with computers, and had experience with internet and online platforms. This was important since previous research suggests that the cognitive load for older adults who are new to computer technology will be higher while performing different tasks, inhibiting their optimum performance [87]. For the same reason, we designed our web-based app to be simple. Since prior literature suggests privacy settings are difficult for older adults to locate and navigate through [11], the control mechanisms in our application were simple radio buttons (for choosing not to disclose) or text boxes (to enter information for disclosure). However, our recruitment strategy and the design of our app may limit the generalizability of our results to older adults who have experience with technology. Further research may also need to be done with applications that are designed with more complexity.

Furthermore, we studied older and younger adults' privacy decision making only in the context of financial applications. Younger adults might not value a financial planning app as much as older adults. To evaluate the generalizability of our findings, future studies should investigate different domains such as health, entertainment, dating and socialization, etc. However, we anticipate that the underlying finding that heuristics can kick in to influence perceptions of sensitivity may still hold for domains with which the users are less familiar. Thus, the model and mechanisms we uncovered can be explored in these other domains.

We focused on young and old adult age brackets, but future research should expand to include a wider range of ages. Furthermore, the majority of our participants were females, and therefore, we controlled for gender in our analysis. While the higher-level objective of this study was to promote inclusion, our limited resources prevented us from recruiting a thoroughly inclusive sample in terms of gender, ethnic, and racial identities. We call for future research to attend to all the population and ensure a representative sample.

7 CONCLUSION

In this paper, rather than focusing on *what* are the age-related differences in privacy, we focused on the *sources* of such differences. We studied the decision-making processes of younger and older adults in the context of a financial app. In line with psychology literature, we found that younger adults heavily rely on heuristics whereas older adults are more likely to be calculus-driven thinkers. However, the heuristics impacted younger adults' decision-making in an unexpected way; rather than having a direct impact on disclosure, reliance on heuristics actually altered the perceived sensitivity of various pieces of personal information. Understanding these underlying mechanisms of privacy decisions can inform the design of digital products and help product developers and designers better support the diverse privacy decision-making processes of their various users.

REFERENCES

[1] Alessandro Acquisti. 2004. Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM conference on Electronic commerce*. 21–29.

[2] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347, 6221 (2015), 509–514.

[3] Alessandro Acquisti and Jens Grossklags. 2005. Privacy and rationality in individual decision making. *IEEE security & privacy* 3, 1 (2005), 26–33.

[4] Alessandro Acquisti and Jens Grossklags. 2007. What can behavioral economics teach us about privacy. *Digital privacy: theory, technologies and practices* 18 (2007), 363–377.

[5] Reza Ghaiumy Anaraky, Bart P Knijnenburg, and Marten Risius. 2020. Exacerbating Mindless Compliance: The Danger of Justifications during Privacy Decision Making in the Context of Facebook Applications. *AIS Transactions on Human-Computer Interaction* 12, 2 (2020), 70–95.

[6] Reza Ghaiumy Anaraky, Tahereh Nabizadeh, Bart P Knijnenburg, and Marten Risius. 2018. Reducing Default and Framing Effects in Privacy Decision-Making. *Proceedings of the Special Interest Group On Humancomputer Interaction* (2018).

[7] Perrin Andrew Anderson, Monica. 2017. *The U.S. Joins Other Countries With Large Aging Populations.* https://www.pewresearch.org/internet/2017/05/17/technology-use-among-seniors/

[8] Susan B Barnes. 2006. A privacy paradox: Social networking in the United States. *First Monday* (2006).

[9] Ryan Best and Neil Charness. 2015. Age differences in the effect of framing on risky choice: A meta-analysis. *Psychology and aging* 30, 3 (2015), 688.

[10] Jeremy Birnholtz and McKenzie Jones-Rounds. 2010. Independence and interaction: understanding seniors' privacy and awareness needs for aging in place. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 143–152.

[11] Petter Bae Brandtzæg, Marika Lüders, and Jan Håvard Skjetne. 2010. Too many Facebook "friends"? Content sharing and sociability versus the need for privacy in social network sites. *Intl. Journal of Human–Computer Interaction* 26, 11-12 (2010), 1006–1030.

[12] Alexandra Brown, J Michael Collins, Maximilian D Schmeiser, and Carly Urban. 2014. State mandated financial education and the credit behavior of young adults. (2014).

[13] US Census Bureau. [n.d.]. Historical Living Arrangements of Adults. https://www.census.gov/data/tables/time-series/demo/families/adults.html Section: Government.

[14] Kaileigh A Byrne and Reza Ghaiumy Anaraky. 2019. Strive to Win or Not to Lose? Age-Related Differences in Framing Effects on Effort-Based Decision-Making. *The Journals of Gerontology: Series B* (2019).

[15] J Alberto Castañeda and Francisco J Montoro. 2007. The effect of Internet general privacy concern on customer behavior. *Electronic Commerce Research* 7, 2 (2007), 117–141.

[16] Eve M Caudill and Patrick E Murphy. 2000. Consumer online privacy: Legal and ethical issues. *Journal of Public Policy & Marketing* 19, 1 (2000), 7–19.

[17] Rajarshi Chakraborty, Claire Vishik, and H Raghav Rao. 2013. Privacy preserving actions of older adults on social media: Exploring the behavior of opting out of information sharing. *Decision Support Systems* 55, 4 (2013), 948–956.

[18] Neil Charness, Mark C Fox, and Ainsley L Mitchum. 2011. Life-span cognition and information technology. (2011).

[19] Feinian Chen, Patrick J Curran, Kenneth A Bollen, James Kirby, and Pamela Paxton. 2008. An empirical evaluation of the use of fixed cutoff points in RMSEA test statistic in structural equation models. *Sociological methods & research* 36, 4 (2008), 462–494.

[20] Jane Chung, George Demiris, and Hilaire J Thompson. 2016. Ethical considerations regarding the use of smart home technologies for older adults: an integrative review. *Annual review of nursing research* 34, 1 (2016), 155–181.

[21] Lynne Coventry and Pam Briggs. 2016. Mobile technology for older adults: Protector, motivator or threat?. In *International Conference on Human Aspects of IT for the Aged Population*. Springer, 424–434.

[22] Lee J Cronbach. 1951. Coefficient alpha and the internal structure of tests. *psychometrika* 16, 3 (1951), 297–334.

[23] Mary J Culnan and Pamela K Armstrong. 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science* 10, 1 (1999), 104–115.

[24] Mary J Culnan and Robert J Bies. 2003. Consumer privacy: Balancing economic and justice considerations. *Journal of social issues* 59, 2 (2003), 323–342.

[25] Louise Cummings. 2014. The "trust" heuristic: Arguments from authority in public health. *Health Communication* 29, 10 (2014), 1043–1056.

[26] Sara J Czaja, Neil Charness, Arthur D Fisk, Christopher Hertzog, Sankaran N Nair, Wendy A Rogers, and Joseph Sharit. 2006. Factors predicting the use of technology: Findings from the center for research and education on aging and technology enhancement (CREATE). *Psychology and aging* 21, 2 (2006), 333.

[27] Nathaniel D Daw, Yael Niv, and Peter Dayan. 2005. Uncertainty-based competition between prefrontal and dorsolateral striatal systems for behavioral control. *Nature neuroscience* 8, 12 (2005), 1704–1711.

[28] Carlo de Bassa Scheresberg. 2013. Financial literacy and financial behavior among young adults: Evidence and implications. *Numeracy* 6, 2 (2013), 5.

[29] Tamara Dinev, Massimo Bellotto, Paul Hart, Vincenzo Russo, Ilaria Serra, and Christian Colautti. 2006. Privacy calculus model in e-commerce–a study of Italy and the United States. *European Journal of Information Systems* 15, 4 (2006), 389–402.

[30] Tamara Dinev and Paul Hart. 2006. An extended privacy calculus model for e-commerce transactions. *Information systems research* 17, 1 (2006), 61–80.

[31] Kenji Doya, Kazuyuki Samejima, Ken-ichi Katagiri, and Mitsuo Kawato. 2002. Multiple model-based reinforcement learning. *Neural computation* 14, 6 (2002), 1347–1369.

[32] Ben Eppinger, Maik Walter, Hauke R Heekeren, and Shu-Chen Li. 2013. Of goals and habits: age-related and individual differences in goal-directed decision-making. *Frontiers in neuroscience* 7 (2013), 253.

[33] AD Fisk and Rogers WA. [n.d.]. Charness N./Czaja SJ/Sharit J.(2009): Designing for older adults. Principles and creative human factor approaches.

[34] Sandra Freitas, Mário R Simões, Lara Alves, and Isabel Santana. 2011. Montreal Cognitive Assessment (MoCA): normative study for the Portuguese population. *Journal of clinical and experimental neuropsychology* 33, 9 (2011), 989–996.

[35] Alisa Frik, Julia Bernd, Noura Alomar, and Serge Egelman. 2020. A qualitative model of older adults' contextual decision-making about information sharing. In *Workshop on the Economics of Information Security (WEIS 2020)*.

[36] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce Lee, Florian Schaub, and Serge Egelman. 2019. Privacy and security threat models and mitigation strategies of older adults. In *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*.

[37] Jan Gläscher, Nathaniel Daw, Peter Dayan, and John P O'Doherty. 2010. States versus rewards: dissociable neural prediction error signals underlying model-based and model-free reinforcement learning. *Neuron* 66, 4 (2010), 585–595.

[38] Zepeng Gong, Ziqiang Han, Xudan Li, Chao Yu, and Jan D Reinhardt. 2019. Factors influencing the adoption of online health consultation services: the role of subjective norm, trust, perceived benefit and offline habit. *Frontiers in Public Health* 7 (2019), 286.

[39] Peter Gregor, Alan F Newell, and Mary Zajicek. 2002. Designing for dynamic diversity: interfaces for older people. In *Proceedings of the fifth international ACM conference on Assistive technologies*. 151–156.

[40] Chris Jay Hoofnagle, Jennifer King, Su Li, and Joseph Turow. 2010. How different are young adults from older adults when it comes to information privacy attitudes and policies? *Available at SSRN 1589864* (2010).

[41] Dominik Hornung, Claudia Müller, Irina Shklovski, Timo Jakobi, and Volker Wulf. 2017. Navigating relationships and boundaries: Concerns around ICT-uptake for elderly people. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 7057–7069.

[42] Cheng-Kui Huang, Shin-Horng Chen, Chia-Pei Tang, and Hsin-Ying Huang. 2019. A trade-off dual-factor model to investigate discontinuous intention of health app users: From the perspective of information disclosure. *Journal of Biomedical Informatics* 100 (2019), 103302.

[43] Janis E Jacobs and Paul A Klaczynski. 2002. The development of judgment and decision making during childhood and adolescence. *Current directions in psychological science* 11, 4 (2002), 145–149.

[44] Sirkka L Jarvenpaa, Noam Tractinsky, and Michael Vitale. 2000. Consumer trust in an Internet store. *Information technology and management* 1, 1-2 (2000), 45–71.

[45] Leslie K John, Alessandro Acquisti, and George Loewenstein. 2011. Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of consumer research* 37, 5 (2011), 858–873.

[46] Eric J Johnson, Steven Bellman, and Gerald L Lohse. 2002. Defaults, framing and privacy: Why opting in-opting out. *Marketing Letters* 13, 1 (2002), 5–15.

[47] Anika K Josef, David Richter, Gregory R Samanez-Larkin, Gert G Wagner, Ralph Hertwig, and Rui Mata. 2016. Stability and change in risk-taking propensity across the adult life span. *Journal of personality and social psychology* 111, 3 (2016), 430.

[48] Sidney M Jourard. 1961. Age trends in self-disclosure. *Merrill-Palmer Quarterly of Behavior and Development* 7, 3 (1961), 191–197.

[49] Bruce E Kaufman. 1999. Emotional arousal as a source of bounded rationality. *Journal of Economic Behavior & Organization* 38, 2 (1999), 135–144.

[50] Mark J Keith, Samuel C Thompson, Joanne Hale, Paul Benjamin Lowry, and Chapman Greer. 2013. Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International journal of human-computer studies* 71, 12 (2013), 1163–1173.

[51] Tom W Kirkman. 1996. Statistics to use. *http://www. physics. csbsju. edu/stats/* (1996).

[52] Bart Knijnenburg and Hongxia Jin. 2013. The persuasive effect of privacy recommendations for location sharing services. *Available at SSRN 2399725* (2013).

[53] Bart Knijnenburg, Elaine Raybourn, David Cherry, Daricia Wilkinson, Saadhika Sivakumar, and Henry Sloan. 2017. Death to the Privacy Calculus? *Available at SSRN 2923806* (2017).

[54] Bart Piet Knijnenburg, Alfred Kobsa, and Hongxia Jin. 2013. Counteracting the negative effect of form auto-completion on the privacy calculus. (2013).

[55] Bran Knowles and Vicki L Hanson. 2018. The wisdom of older technology (non) users. *Commun. ACM* 61, 3 (2018), 72–77.

[56] Spyros Kokolakis. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security* 64 (2017), 122–134.

[57] Hanna Krasnova and Natasha F Veltri. 2010. Privacy calculus on social networking sites: Explorative evidence from Germany and USA. In *2010 43rd Hawaii international conference on system sciences*. IEEE, 1–10.

[58] Hanna Krasnova, Natasha F Veltri, and Oliver Günther. 2012. Self-disclosure and privacy calculus on social networking sites: The role of culture. *Business & Information Systems Engineering* 4, 3 (2012), 127–135.

[59] Jess Kropczynski, Zaina Aljallad, Nathan Jeffrey Elrod, Heather Lipford, and Pamela J Wisniewski. 2021. Towards Building Community Collective Efficacy for Managing Digital Privacy and Security within Older Adult Communities. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3 (2021), 1–27.

[60] AJ Larner. 2012. Screening utility of the Montreal Cognitive Assessment (MoCA): in place of-or as well as-the MMSE? *International Psychogeriatrics* 24, 3 (2012), 391.

[61] Robert S Laufer and Maxine Wolfe. 1977. Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of social Issues* 33, 3 (1977), 22–42.

[62] Roy J Lewicki and Chad Brinsfield. 2011. Framing trust: trust as a heuristic. *Framing matters: Perspectives on negotiation research and practice in communication* (2011), 110–135.

[63] Michael Lewis-Beck, Alan E Bryman, and Tim Futing Liao. 2003. *The Sage encyclopedia of social science research methods*. Sage Publications.

[64] He Li, Jing Wu, Yiwen Gao, and Yao Shi. 2016. Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *International journal of medical informatics* 88 (2016), 8–17.

[65] Ulman Lindenberger, Martin Lövdén, Michael Schellenbach, Shu-Chen Li, and Antonio Krüger. 2008. Psychological principles of successful aging technologies: A mini-review. *Gerontology* 54, 1 (2008), 59–68.

[66] Linda Little, Pamela Briggs, and Lynne Coventry. 2011. Who knows about me? An analysis of age-related disclosure preferences. (2011).

[67] George F Loewenstein, Elke U Weber, Christopher K Hsee, and Ned Welch. 2001. Risk as feelings. *Psychological bulletin* 127, 2 (2001), 267.

[68] Miguel Malheiros, Sören Preibusch, and M Angela Sasse. 2013. "Fairly truthful": The impact of perceived effort, fairness, relevance, and sensitivity on personal data disclosure. In *International Conference on Trust and Trustworthy Computing*. Springer, 250–266.

[69] Mara Mather and Laura L Carstensen. 2005. Aging and motivated cognition: The positivity effect in attention and memory. *Trends in cognitive sciences* 9, 10 (2005), 496–502.

[70] Anita Melander-Wikman, Ylva Fältholm, and Gunvor Gard. 2008. Safety vs. privacy: elderly persons' experiences of a mobile safety alarm. *Health & social care in the community* 16, 4 (2008), 337–346.

[71] Miriam J Metzger. 2004. Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of computer-mediated communication* 9, 4 (2004), JCMC942.

[72] Earl K Miller and Jonathan D Cohen. 2001. An integrative theory of prefrontal cortex function. *Annual review of neuroscience* 24, 1 (2001), 167–202.

[73] Peter Millward. 2003. The'grey digital divide': Perception, exclusion and barriers of access to the Internet for older people. *First Monday* (2003).

[74] Caroline Lancelot Miltgen and Dominique Peyrat-Guillard. 2014. Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. *European journal of information systems* 23, 2 (2014), 103–125.

[75] Cristian Morosan and Agnes DeFranco. 2015. Disclosing personal information via hotel apps: A privacy calculus perspective. *International Journal of Hospitality Management* 47 (2015), 120–130.

[76] United Nations. [n.d.]. *Ageing*. https://www.un.org/en/sections/issues-depth/ageing/

[77] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.

[78] US Department of Health, Human Services, et al. 2019. *Administration on aging. 2017 Profile of older Americans.*

[79] Dara O'Neil. 2001. Analysis of Internet users' level of online privacy concerns. *Social Science Computer Review* 19, 1 (2001), 17–31.

[80] Yong Jin Park. 2013. Digital literacy and privacy behavior online. *Communication Research* 40, 2 (2013), 215–236.

[81] Anabel Quan-Haase and Isioma Elueze. 2018. Revisiting the privacy paradox: Concerns and protection strategies in the social media experiences of older adults. In *Proceedings of the 9th International Conference on Social Media and Society*. 150–159.

[82] David R Roalf, Paul J Moberg, Sharon X Xie, David A Wolk, Stephen T Moelter, and Steven E Arnold. 2013. Comparative accuracies of two common screening instruments for classification of Alzheimer's disease, mild cognitive impairment, and healthy aging. *Alzheimer's & Dementia* 9, 5 (2013), 529–537.

[83] Andrew W Roberts, Stella U Ogunwole, Laura Blakeslee, and Megan A Rabe. 2018. *The population 65 years and older in the United States: 2016*. US Department of Commerce, Economics and Statistics Administration, US ....

[84] Wendy A Rogers and Arthur D Fisk. 2010. Toward a psychological science of advanced technology design for older adults. *Journals of Gerontology Series B: Psychological Sciences and Social Sciences* 65, 6 (2010), 645–653.

[85] Wendy A Rogers, Beth Meyer, Neff Walker, and Arthur D Fisk. 1998. Functional limitations to daily living tasks in the aged: A focus group analysis. *Human factors* 40, 1 (1998), 111–125.

[86] John T Scholz and Mark Lubell. 1998. Trust and taxpaying: Testing the heuristic approach to collective action. *American Journal of Political Science* (1998), 398–417.

[87] Joseph Sharit, Sara J Czaja, Mario Hernandez, Yulong Yang, Dolores Perdomo, John E Lewis, Chin Chin Lee, and Sankaran Nair. 2004. An evaluation of performance by older persons on a simulated telecommuting task. *The Journals of Gerontology Series B: Psychological Sciences and Social Sciences* 59, 6 (2004), P305–P316.

[88] Hu Shuijing and Jiang Tao. 2017. An Empirical Study on Digital Privacy Risk of Senior Citizens. In *2017 International Conference on Robots & Intelligent System (ICRIS)*. IEEE, 19–24.

[89] Mart Tacken, Fiorella Marcellini, Heidrun Mollenkopf, Isto Ruoppila, and Zsuzsa Szeman. 2005. Use and acceptance of new technology by older people. Findings of the international MOBILATE survey:'Enhancing mobility in later life'. *Gerontechnology* 3, 3 (2005), 126–137.

[90] Jiang Tao and Hu Shuijing. 2016. The elderly and the big data how older adults deal with digital privacy. In *2016 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS)*. IEEE, 285–288.

[91] John Taylor. 1997. *Introduction to error analysis, the study of uncertainties in physical measurements*.

[92] Kathryn J Thirlaway and Daniel A Heggs. 2005. Interpreting risk messages: Women's responses to a health story. *Health, risk & society* 7, 2 (2005), 107–121.

[93] Evert Van den Broeck, Karolien Poels, and Michel Walrave. 2015. Older and wiser? Facebook use, privacy concern, and privacy protection in the life stages of emerging, young, and middle adulthood. *Social Media+ Society* 1, 2 (2015), 2056305115616149.

[94] Edward Shih-Tse Wang. 2019. Effects of brand awareness and social norms on user-perceived cyber privacy risk. *International Journal of Electronic Commerce* 23, 2 (2019), 272–293.

[95] Le Wang, Hai-Hua Hu, Jie Yan, and Maggie Qiuzhu Mei. 2019. Privacy calculus or heuristic cues? The dual process of privacy decision making on Chinese social media. *Journal of Enterprise Information Management* (2019).

[96] Michele Williams. 2001. In whom we trust: Group membership as an affective context for trust development. *Academy of management review* 26, 3 (2001), 377–396.

[97] Darrell A Worthy, Marissa A Gorlick, Jennifer L Pacheco, David M Schnyer, and W Todd Maddox. 2011. With age comes wisdom: Decision making in younger and older adults. *Psychological science* 22, 11 (2011), 1375–1380.

[98] Feng Xu, Katina Michael, and Xi Chen. 2013. Factors affecting privacy disclosure on social network sites: an integrated model. *Electronic Commerce Research* 13, 2 (2013), 151–168.

[99] Heng Xu, Xin Robert Luo, John M Carroll, and Mary Beth Rosson. 2011. The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision support systems* 51, 1 (2011), 42–52.

[100] Heng Xu, Hock-Hai Teo, and Bernard Tan. 2005. Predicting the adoption of location-based services: the role of trust and perceived privacy risk. *ICIS 2005 proceedings* (2005), 71.

[101] Heng Xu, Hock-Hai Teo, Bernard CY Tan, and Ritu Agarwal. 2009. The role of push-pull technology in privacy calculus: the case of location-based services. *Journal of management information systems* 26, 3 (2009), 135–174.

[102] Eva-Maria Zeissig, Chantal Lidynia, Luisa Vervier, Andera Gadeib, and Martina Ziefle. 2017. Online privacy perceptions of older adults. In *International Conference on Human Aspects of IT for the Aged Population*. Springer, 181–200.

[103] Xing Zhang, Shan Liu, Xing Chen, Lin Wang, Baojun Gao, and Qing Zhu. 2018. Health information privacy concerns, antecedents, and information disclosure intention in online health communities. *Information & Management* 55, 4 (2018), 482–493.

[104] Kathryn Zickuhr, Mary Madden, et al. 2012. Older adults and internet use. *Pew Internet & American Life Project* 6 (2012).

[105] Sonja Zmerli and Tom WG Van der Meer. 2017. *Handbook on political trust*. Edward Elgar Publishing.

8 APPENDIX

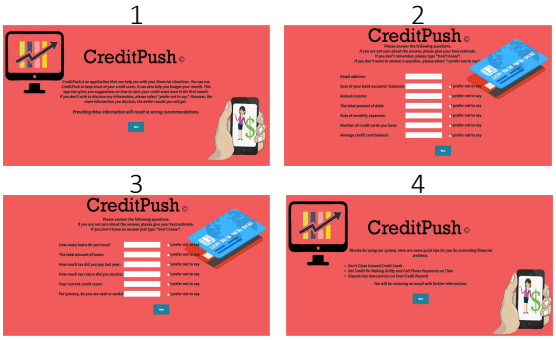


Figure A1: Screenshots of the app. In the first page users gain some information about the app, in the second and third pages they disclose (or withhold) information, and in the last page they receive some feedback and then proceed to the surveys.

Table A1: Descriptive statistics on data-items. Participants were able to disclose or withhold their data. The overall disclosure percentages are reported in this table. Participants were also asked to rate the sensitivity level of each data-item, and specify the extent to which they believe disclosing each data-item would improve the app-generated recommendation quality.

Item	Data items requested from users	Disclosure Percentage (alpha = 0.963)	Mean for Sensitivity (alpha = 0.931)	Mean for Perceived Improvement in Recommendation Quality (alpha = 0.933)
1	Sum of your bank accounts' balances	0.525	2.872	5.223
2	Annual income	0.587	2.648	5.478
3	The total amount of debt	0.737	2.659	5.542
4	Sum of monthly expenses	0.662	2.191	5.500
5	Number of credit cards you have	0.825	1.808	5.202
6	Average credit card balance	0.737	2.382	5.553
7	How many loans do you have?	0.838	2.308	5.468
8	The total amount of loans	0.852	2.531	5.542
9	How much tax did you pay last year	0.602	2.404	4.925
10	How much tax return did you receive	0.691	2.297	4.872
11	Your current credit score	0.617	2.319	5.457
12	For grocery, do you use cash or cards?	0.867	1.361	4.095

Table A2: Trust Items Adopted from Jarvenpaa et al. [44] and Metzger et al. [71]

#	Trust Items
1	I believe CreditPush is trustworthy in handling my information.
2	I believe CreditPush tells the truth and fulfills promises related to the information I provide.
3	I believe CreditPush is predictable and consistent regarding the usage of my information.
4	I believe CreditPush is honest when it comes to using the information I provide.