Share or Protect: Understanding the Interplay of Trust, Privacy Concerns, and Data Sharing Purposes in Health and Well-Being Apps

Agnieszka Kitkowska
agnieszka.kitkowska@ju.se
Jönköping University
Jönköping, Sweden

Farzaneh Karegar
farzaneh.karegar@kau.se
Karlstad University
Sweden

Erik Wästlund
Erik.Wastlund@ju.se
Jönköping University
Sweden

ABSTRACT
The popularity of health and well-being applications is on the rise. These applications often collect and process personal and sensitive information about individuals for different purposes. Nonetheless, users’ freedom of choice around protection and sharing may be compromised, for example, by forwarding such information to third parties without user awareness or control, especially with current developments in AI-based complex data processing technologies. Despite the popularity of health and well-being applications, the purpose of sharing and its interplay with trust, privacy concerns, and their antecedents is seldom explored. The present article addresses this gap by conducting an online study (N = 315), which shows that, generally, people’s sharing preferences depend on their trust and privacy concerns. However, the findings indicate potential differences between male and female participants considering sharing information for the greater good, such as scientific research. Our findings are discussed in light of sociocultural and social role theories of prosocial behavior and previous research. Considering the growing interest in building usable infrastructures for data sharing and user empowerment, practical implications for designers and policymakers are highlighted.

CCS CONCEPTS
• Human-centered computing → Empirical studies in HCI; • Security and privacy → Social aspects of security and privacy.

KEYWORDS
privacy, decision-making, gender, information sharing

1 INTRODUCTION
Health, well-being, and fitness applications use is expected to grow exponentially over the next few years [12, 57, 68]. The evidence suggests that such applications contribute to maintaining a healthy lifestyle and well-being, both physically and mentally [18, 56]; however, the level of their efficiency varies [46]. In order to function correctly, these applications must collect and process specific data about individuals. Most of this data is personal (e.g., email address) and sensitive (e.g., health-related data, such as information collected by wearable sensors—heart rate, sleep patterns). Advances in AI-based technologies, their application in the eHealth domain, the creation of massive datasets, and the complex data flow between entities may, however, under specific circumstances, hamper users’ privacy and their freedom of choice around protection and sharing. As much as such information is required for the apps to function, some might be shared with third parties, such as sister companies, advertisers, or analytical companies. A service provider may be interested, for example, in increasing their revenue by selling or sharing data with advertisers, building a personalized system, gaining insights from data analytics, or similar. However, it is also possible that the service will share data for more benevolent purposes, for instance, with third parties conducting health research for the benefit of all.

The latter could be labeled as sharing for the greater good and classified as a prosocial act. In the European Union (EU) importance of data exchange for the greater good has been recognized by policymakers. As a part of plans for digital Europe, the EU vision is to enable sharing of data, including health-related data, between different public organizations [22], consequently allowing citizens to receive personalized care regardless of location. Although legislation such as Data Governance Act focuses on the data exchange between public organizations [21], other legislative proposals aim to improve data exchange between business and public actors within the EU; for instance, Data Act strives to balance data sharing and better regulate the market, allowing public actors to access and use data [20]. Together with the General Data Protection Regulation (GDPR) [19], all of these legal frameworks aim to give users access and control over their information, make switching between service providers easier, and empower users to make more beneficial decisions. Similar views are also present in the international landscape expanding beyond the EU. For example, the Organisation for Economic Co-operation and Development (OECD) emphasizes the importance of sharing digital information among different actors and ensuring societal (including citizen empowerment, data access, sharing and use) and business (reinforcing trust and stimulating
investment) benefits of such sharing [47]. Taken together, these legal frameworks indicate the demand for changes in the current technologies, including the need for applications to give users easy and greater control over personal information.

To design usable services that provide users with granular and meaningful control, it is necessary to understand their attitudes and behaviors toward sharing information. Past research investigated these issues, but predominantly in the context of sharing information with other users on social networks or sharing with service providers [33, 36, 43]. However, not much attention has been given to investigating attitudes toward sharing with third parties, simultaneously considering different sharing purposes. The present research aims to address this gap, and investigate sharing health and well-being-related information with third parties, focusing on four purposes of the shared information: personalization, application improvement, improvement of privacy and security, and scientific research. Moreover, considering the rising number of users of health and well-being applications, the present research focuses on the health context to zoom into sharing potentially sensitive information in the hope of identifying whether such sharing could be considered prosocial behavior. Among others, the results of the present study confirm that overall, people tend to behave rationally, in an economic sense, regarding sharing health-related information with third parties. Their sharing behavior is predicted by trust and privacy concerns—with lower trust and greater concerns, people tend to share less. However, this relationship is moderated by gender in the context of sharing information for scientific research. We discuss these and other findings against the prosocial and gender role theories, as well as reflect on the potential practical and theoretical implications of the present research.

The rest of the paper is structured as follows. First, the Background section presents an overview of the theoretical foundations of concepts investigated in the present research and relevant work. Next, the Method section presents the research questions addressed in the paper and explains the methodological approach undertaken to answer these questions, including the study design process and conceptual model. Additionally, the section describes the participants. The Results section follows it, providing insights into the studied variables and statistical analysis used to answer the research questions. Next, the Discussion section summarizes the research findings, elaborating on the theoretical and practical implications of the study results. Lastly, concluding remarks are presented in the Conclusion section.

2 BACKGROUND

People’s sharing activities may relate to prosocial behaviors. Such behaviors may differ depending on gender, the different recipients of shared information, and sharing purposes. In this section, we present an overview of prosocial behaviors and elaborate on information sharing in the digital space, considering privacy and security concerns related to information sharing.

2.1 Prosocial behavior and gender

Prosocial behaviors aim to benefit others. Therefore they include helping, donating to charity, and sharing [28], and may differ depending on demographic characteristics, such as gender. Gender can be defined as “[referring] to the characteristics of women, men, girls, and boys that are socially constructed. This includes norms, behaviors, and roles associated with being a woman, man, girl, or boy, as well as relationships with each other. As a social construct, gender varies from society to society and can change over time.” [74]. It is common to assume that gender may relate to people’s attitudes and behaviors. Often, people mistakenly relate gender differences to sex-based division. Research recognizes different theoretical explanations for gender differences, of which one prominent is the sociocultural theory, which assumes that the social division of gender roles drives other gender differences.

The gender-dependent differences can be associated with gender stereotypes. For instance, the two dimensions labeled as agentic (characterized by traits such as master-fullness, competitiveness, dominance, assertiveness) and communal (characterized by traits such as unselfish, emotional, friendliness, caring) [15, 16]. Accordingly, men are more likely to be agentic, and women are more likely to be communal. Still, past research implies that people internalize their gender roles [73], meaning people tend to apply internalized gender as personal gender identities. As a result, it is the self-conceptualizations of gender, not the reported gender, that correlate with communal or agentic division. Gender role internalization is a premise of sociocultural theory that assumes that gender role beliefs, together with self-regulation and social regulation, influence cognition, affect, or behavior [16]. Additionally, gender roles are thought to be affected by biological predispositions related to hormonal changes [16].

Considering prosocial behavior and people-things dimensions, men seem more thing-oriented than women and much less people-oriented [42]. Males help more, particularly in dangerous circumstances (e.g., danger-involving situations), and express hero-like behaviors when there is an audience (e.g., bystanders) [34]. On the other hand, females tend to help more in situations where the stereotypical female role is associated with behavior, e.g., helping a child in distress [34]. Also, there are indications that females are more altruistic, particularly in sharing or giving. For instance, females tend to donate more money and time than males [60].

The risk-taking between males and females tends to differ. Women are less likely than men to participate in risk-eliciting behavior, e.g., drug or alcohol abuse, criminal activities [17, 30]. Similarly, they are more risk averse in gambling [17]. Moreover, considering the positive domain—when choices offer substantial gain but low cost—women seem to engage more in such behaviors, recognizing and valuing positive consequences [30].

2.1.1 Privacy & security and gender. Some studies indicate the association between gender and security and privacy beliefs and behaviors. For instance, gender may affect self-disclosure of information [40, 55, 58], privacy concerns [8], and protection strategies [48]. In addition, gender may influence the use of private browsing [29] and two-factor authentication [53], how security warnings are interpreted [2], and how security attitudes are held [23].

Moreover, Wei et al. [72] show potential security and privacy stereotypes and explore beliefs about gender stereotypes related to security and privacy behaviors and personal characteristics. Even though several participants attributed stereotypes to biological reasons, many believed that stereotypes were valid based on other
factors [72]. A significant correlation existed between stereotype beliefs and the gender and level of sexism of participants. Participants generally considered women more emotional and susceptible and to take poorer security and privacy measures than men. On the other hand, participants thought men were more likely to take protective measures and engage with security and privacy topics [72].

2.2 Information sharing

People share information about themselves in digital space for many reasons. Research indicates that sharing on social networks might be related to prosocial behavior. For instance, an online survey collecting data about social media sharing indicated that altruism significantly affects knowledge sharing [43]. The prosocial, altruistic motivations for sharing information online were also identified in the context of fake news and the Covid-19 pandemic [3], and in sharing tourism-related advertisements on Facebook [51]. However, such data sharing—when an individual discloses information about themselves directly, purposefully, and, in most cases, knowingly—is different from data sharing with third parties.

Considering health-related data sharing, there is a large body of knowledge about patients and medical research. For instance, a survey of EU citizens shows that people prefer to share their electronic records with healthcare professionals but oppose sharing such data with third parties (e.g., private sector) [49]. Moreover, people have reservations about sharing their health data with academic research communities [49]. Trinidad et al. [69] defined the public’s comfort with sharing health data with third-party commercial companies for patient purposes (i.e., to improve care, diagnosis, or treatment) and business purposes (i.e., the sale of de-identified data for artificial intelligence efforts) and how this comfort is associated with demographic factors and privacy concerns. The public is more willing to share health data with third-party commercial companies for patient purposes than business purposes.

People seem to have positive attitudes towards using their health-related information beyond the treatment [62], but conditionally. According to systematic reviews, people agree with the secondary use of their health information, as long as such use is to bring a positive outcome—contribute to the greater good [1, 62, 65]. This is particularly valid when sharing for research, policy, and planning, and the result of sharing will benefit the public. The willingness to share health information was also associated with personal responsibility and obligation to help others [65], which aligns with prosocial behavior discussed in Section 2.1.

2.2.1 Sharing and user-generated data. People trace their activities using wearable devices and may improve their health by tracking personal data, e.g., step count and sleep quality, and monitoring medical conditions (e.g., diabetes). Users can also share the health and fitness information collected by wearables with different people and organizations through various communication channels (e.g., social networks and external fitness apps) for different purposes (e.g., meeting fitness goals with different people and organizations). Despite the growing use of technologies that collect health-related data, to the best of our knowledge, little is known about end-users’ attitudes toward sharing such user-generated data with third parties. In the context of mobile apps for depression management, research indicates a willingness to share with professionals (e.g., physicians, psychotherapists), particularly among males [31]. However, people prefer to keep such data private from family members or friends. Although people do not mind sharing with health care providers, desires that drive such sharing decisions are rather self-centered, e.g., sharing to foster greater health care [39].

Some research investigated users’ sharing attitudes and behaviors in the context of wearables (e.g., [27, 52, 54]), considering the types of recipients of the data people share, and how the data would be used if shared. There is no convergence between the results of the different studies. Prasad et al. [52] found that people share certain health information with specific third parties more often than they do with the public, but their results may not apply to experienced users. In other words, people are more willing to share if they perceive benefits in sharing, especially when it comes to exchanging information with specific third parties, as opposed to the public [52]. Moreover, people are way more concerned about sharing data with the general public than sharing it with other study participants and researchers, regardless of whether the shared data is anonymized or pseudonymized [54]. Those surveyed in [27] were most comfortable sharing their data with the tracker and their friends, less so with coworkers and employers, and least comfortable sharing with strangers (the public, insurance companies, and advertisers).

Another research strain looked at mobile app permissions, focusing on usability and sharing preferences (e.g., [26, 41, 66, 67]). For instance, researchers investigated the reasons why users allow and do not allow different permissions [66]. The app functionality was the highest scoring factor [66]. Other research examined the more specific reasons for app permissions, providing users with explanations of why different permission is requested [67]. Most users were willing to allow permission access if they personally benefited [67]. Still, to the best of our knowledge, past studies did not explicitly investigate sharing with third parties, providing users with control and choice around disclosures.

2.2.2 APCO and health-related information. The APCO macro model is one framework for analyzing privacy-related attitudes and behaviors (Antecedents → Privacy concerns → Outcomes). Based on the literature review, the framework incorporates knowledge from behavioral and cognitive sciences [14, 64]. In short, the model assumes that privacy concerns are central to privacy decision-making and directly influence behavioral outcomes (e.g., information disclosure). However, other factors, such as cultural background, demographics, personality, or previous experiences, may affect privacy concerns. The APCO supposes privacy calculus (cost and benefit analysis) may significantly affect privacy concerns. Moreover, trust affects privacy concerns directly or indirectly influences behavioral outcomes. Lastly, the relationships between latent constructs and behavioral outcomes are moderated by other factors, e.g., biases and heuristics, cognitive efforts, or peripheral cues. The APCO framework was validated in the research [9]. For instance, antecedents of privacy concerns, including gender and

1Latent construct, also referred to as latent variable, is a theoretical entity or construct that is “used to explain one or more manifest variables. Latent variables cannot be directly observed or measured but rather are approximated through various measures presumed to assess part of the given construct” [4].
previous privacy experience, were shown to have a strong relationship, as well as privacy concerns and behavioral outcomes (in this instance, protection behavior) [9].

**Privacy concerns.** People express privacy-related concerns and reservations about sharing health data. In their review of sharing health information for research purposes, Aitken et al. list conditions of why individuals are willing to share [1]. The leading reason is confidentiality, which is frequently associated with anonymization. People are less concerned about the quantitative information about their health, but their worries increase considering qualitative information. Next to confidentiality, people are worried about the security of their health data, considering the possible security issues due to systems’ failure and human errors [1]. Another review pointed out that people are aware of potential risks related to data sharing, e.g., unauthorized access, access without explicit consent, re-identification, data aggregation to disadvantage specific groups, and governmental access to health information [65].

People are also concerned about harms, e.g., identity theft, stigmatization in the clinical setting, potentially adverse effects on employment, insurance cost, and community embarrassment [65]. Another review indicated that the reuse of health data for research could be consent-less as long as the data is anonymized [62]. However, the opinions are less uniform considering the geographic distributions of studied samples or purposes for which health data is to be shared. Anonymity emerges as important in the study conducted with people living with health conditions prone to stigmatization [10]. The participants want control over anonymity, which could facilitate sharing with third parties. Without anonymity, participants worry that their information could be linked to and affect their “real life,” both social and professional. Hence, instruments to limit sharing of personal information with specific recipients are of interest.

**Trust.** Trust is another factor affecting privacy concerns and behavioral outcomes. Trust issues surface in past research considering sharing health-related information in the UK [65]. People seem concerned about whether they can trust National Health Service (NHS) regarding the security and data handling processes. Similarly, studies investigating mobile health applications mention privacy, security, and trust issues. For instance, Peng et al. reports that people are not keen on sharing or seeing shared information from mobile health applications on social media [50]. Their findings revealed concerns about trust and access to shared information by third parties, particularly insurance companies or advertisers.

**Gender.** The differences between individuals, depending on gender and privacy and security attitudes, affect behavior, as described in Section 2.1. Moreover, the direct relationship between privacy concerns and gender was found in the research on the health information privacy concerns (HIPC) scale, proposed by Fox and James [24]. Their study indicated that men have more privacy concerns regarding health-related data than females.

**Experience.** Past research indicates that privacy concerns differ between people, and those who experienced online privacy violations have greater privacy concerns than those who did not [45, 63]. Negative previous experiences, such as hacking, result in decreased levels of trust, regardless of the level of privacy concerns [6]. Experiences of unauthorized sharing violate trust even more severely [6]. In the context of health information, findings are similar, indicating that previous experiences of privacy invasions increase health data privacy concerns [7]. Similarly, the results of a study of people with mental health conditions showed that privacy victimization experience (including the experience of being a victim of someone known and unknown and misuse of information about a victim) has a positive relationship with privacy concerns [75]. On the other hand, another research does not reveal a significant relationship between a previous experience (privacy invasion) and health information privacy concerns [24].

### 3 Method

Taking into account the previous research on privacy and sharing attitudes and behaviors, as well as the theoretical assumptions related to drivers of prosocial behaviors and sociocultural theory, in the present research, we desire to gain more knowledge about people’s sharing behaviors. We focus on the context of sharing user-generated health and well-being data. Specifically, we focus on sharing with third parties for specific purposes since this topic is underresearched to the best of our knowledge. Moreover, a recent review from Simpson et al. recommended sharing user-generated data with third parties as a topic that requires more investigation [61].

Therefore, in the present research, we aim to answer the following questions:

**RQ1** What is the relationship between privacy concerns, trust, and sharing information for different purposes with third parties in the context of using health and well-being applications?

**RQ2** Does this relationship differ, taking into account antecedents of privacy concerns, such as demographic characteristics (males vs. females) and previous experiences (experiences with privacy breaches)?

To answer these research questions, we apply the APCO framework. However, investigating all factors included in the model would be difficult and could render misleading results due to a large number of variables. We select factors most relevant to the posited research questions. Figure 1 visualizes the current research approach, assuming that trust has a direct relationship with sharing but also an indirect relationship mediated by privacy concerns. We suppose that these relationships might be moderated by either gender or previous experiences of privacy or security breaches.

---

**Figure 1: Conceptual model of the present study.**
3.1 Study design
The present research is part of a larger project investigating sharing preferences among different demographic groups and application design, focusing on the geographic area of EEA, UK, and USA. The larger project, which is not the focus of the present paper, consisted of 700 participants in total. However, in this article, we only report on the latent constructs (privacy concerns, trust, security concerns, perceived ability to control), demographic dependencies (gender), previous experiences (privacy and security breaches), and one of the investigated sharing types—sharing with third parties for specific purposes. Therefore, in the present research, we present only half of the sample (see more details in Section 3.3), relevant to the present article’s research questions.

To address our research questions, we designed an online study distributed to participants between October and November 2022. The study was implemented with easily customizable SoSci software, enabling experimental design. The software is installed on the local university server and maintained by the Karlstad University IT department. We used the Prolific platform to distribute the study to participants. First, we ran a pilot study with 70 participants. The purpose of the pilot was to identify possible flows in the study design without conducting the full data analysis. The study contained a comment section (allowing text input) became a useful tool to identify whether participants had any difficulties understanding the study, but this was not the case. Respondents noticed some spelling mistakes in the study and that one question did not display correctly. We used that information to correct any mistakes. Each participant who completed the study (both the pilot and the main study) received GBP 2.40. The average completion time for the study was approx. 9 minutes.

Before commencing, all participants were presented with informed consent, which they needed to acknowledge. The study contained the following phases.

**Interactive task.** We presented participants with a made-up scenario. They were asked to imagine using a health and well-being application for over a year that provides insights into managing their health and what steps they should take to improve their well-being. According to the scenario, the application would automatically collect participants’ information (e.g., their steps and location) and participants could self-report their physical and mental health. Then we asked them to change privacy settings in this app. Next, we presented participants with a fictitious application, where participants were to decide on their sharing preferences for the information that this application shares with third parties. We asked participants about sharing with five different third parties (private local, private abroad, a local governmental organization, a governmental organization within the EU, and a governmental organization outside of the EU). For each third party, participants could choose which sharing purposes they agree to disclose to the given third party. Furthermore, we offered participants the option of specifying their preferences regarding sharing purposes, regardless of the third party, and not specifying their preferences at all.

Appendix A.1 presents the exact questions participants answered when completing the interactive task.

In the present article, we do not report on sharing with specific third parties, as we are only interested in differences considering sharing purposes. The different sharing purposes used in the present article are as follows: (a) to improve how this application works; (b) to improve and personalize my experience; (c) to contribute to scientific research; (d) to improve the application’s privacy & security.

**Measurement of latent constructs.** After interacting with the fictitious application, participants were asked a series of questions containing measurements of the latent constructs of interest for the current research: privacy concerns, security concerns, previous experiences of privacy or security breaches, and users’ trust. We also asked some ad hoc questions about the perceived ability to control. Detailed questions regarding each construct, along with ad hoc questions, can be found in Appendix A.2.

**Measurement of demographic characteristics.** After assessing the attitudinal constructs, we asked participants demographic questions (see Appendix A.3), e.g., age, country of residence, gender, education, and employment.

3.2 Ethical vetting
The research proposal underwent an ethical review from the Swedish National Ethical Authority (Etikprövningsmyndigheten), reference number 2022-01343-01. The review board determined that this work would not expose participants to any potential risks. To comply with the legal requirements, the researchers made an effort to minimize data collection and reduce the probability of identifying an individual.

3.3 Participants
The study was distributed online using Prolific Academic. To participate in the study, respondents had to be at least 18 years old and speak English. Because of the study design (i.e., the categorization of third parties with whom they could decide whether to share their data for different purposes), we used geographical screening and collected responses only from participants located in the countries from European Economic Area (EEA), the UK, and the USA. In total, we gathered 700 participants. However, in the present article, we report on findings that consider only the participants that specified their preference for sharing purposes, i.e., either specified their sharing purposes for specific third parties or regardless of third parties as part of the interactive task described in Section 3.1, which reduced the sample size to \( N = 317 \). Because we wanted to use gender as one of the predictor variables, we removed two cases that selected “Other” or “Prefer not to say” options when asked to describe their gender. Hence, the final sample size is \( N = 315 \).

Approximately half of the participants described themselves as females ($n = 164$). Almost half of the participants belonged to the younger generation, in the age group between 18 and 29 years old ($n = 139$). The next large age cohort consisted of participants 30-39 years old ($n = 79$). The participants’ geographical distribution was diverse, primarily due to the pre-screening of the study. The study link was distributed to participants living in the EEA countries (https://www.prolific.co/)
Table 1: Participants’ details.

<table>
<thead>
<tr>
<th>Demographic</th>
<th>N</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>151</td>
<td>47.9</td>
</tr>
<tr>
<td>Female</td>
<td>164</td>
<td>52.1</td>
</tr>
<tr>
<td>Age</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18-29</td>
<td>139</td>
<td>44.1</td>
</tr>
<tr>
<td>30-39</td>
<td>79</td>
<td>25.1</td>
</tr>
<tr>
<td>40-49</td>
<td>41</td>
<td>13.0</td>
</tr>
<tr>
<td>50-59</td>
<td>35</td>
<td>11.1</td>
</tr>
<tr>
<td>over 60</td>
<td>21</td>
<td>6.7</td>
</tr>
<tr>
<td>Country</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UK</td>
<td>84</td>
<td>26.7</td>
</tr>
<tr>
<td>Portugal</td>
<td>55</td>
<td>17.5</td>
</tr>
<tr>
<td>Poland</td>
<td>52</td>
<td>16.5</td>
</tr>
<tr>
<td>Italy</td>
<td>29</td>
<td>9.2</td>
</tr>
<tr>
<td>Greece</td>
<td>21</td>
<td>6.7</td>
</tr>
<tr>
<td>Other</td>
<td>74</td>
<td>23.4</td>
</tr>
<tr>
<td>Employment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>University student</td>
<td>73</td>
<td>23.2</td>
</tr>
<tr>
<td>Employee/working</td>
<td>196</td>
<td>62.2</td>
</tr>
<tr>
<td>Unemployed</td>
<td>19</td>
<td>6.0</td>
</tr>
<tr>
<td>Pensioner</td>
<td>12</td>
<td>3.8</td>
</tr>
<tr>
<td>Other</td>
<td>15</td>
<td>4.8</td>
</tr>
<tr>
<td>Education</td>
<td></td>
<td></td>
</tr>
<tr>
<td>High school</td>
<td>60</td>
<td>19.0</td>
</tr>
<tr>
<td>Bachelor’s degree</td>
<td>94</td>
<td>29.8</td>
</tr>
<tr>
<td>Junior high diploma</td>
<td>13</td>
<td>4.1</td>
</tr>
<tr>
<td>Certificate of secondary education</td>
<td>15</td>
<td>4.8</td>
</tr>
<tr>
<td>Vocational secondary certification</td>
<td>32</td>
<td>10.2</td>
</tr>
<tr>
<td>Master’s degree or higher</td>
<td>96</td>
<td>30.5</td>
</tr>
<tr>
<td>Other qualification</td>
<td>5</td>
<td>1.6</td>
</tr>
</tbody>
</table>

and UK and USA. Over a quarter of participants were from the UK (n = 84), and participants from Portugal (n = 55) and Poland (n = 52) created the next two largest geographical clusters. The majority of participants were employed/working (n = 196), and had higher education (n = 94 had Bachelor’s degree, and n = 96 had a Master’s degree or higher). The details of participants’ demographics are presented in Table 1.

4 RESULTS

To answer the research questions, we used statistical analysis, including parametric and non-parametric tests. We used t-tests and path analysis. Before presenting the results, we report on variables used in the analysis.

4.1 Studied variables

We looked at associations between individual characteristics and latent constructs. Gender was used as a variable to assess differences between males (n = 151) and females (n = 164). Previous experience was used as another variable to assess differences between people who experienced privacy or security breaches (n = 77) and those who did not experience them (n = 238). We used the sum of sharing scores as a behavioral outcome variable for each sharing purpose. These scores were transformed using log transformation. Next, we describe the latent constructs capturing privacy concerns, security concerns, trust, and perceived control as attitudinal factors used in our model.

Privacy concerns. We measured privacy concerns using an instrument acquired from [5] (a shorter version of a widely used instrument proposed by [44]). We investigated the two dimensions of privacy concerns: collection and secondary use, measured with six items. The level of concern was measured on a Likert scale ranging from 1 (very low) to 5 (very high). To ensure the instrument’s reliability, we conducted Principal Component Analysis (PCA) with varimax rotation. All items loaded into two factors corresponding to the expected two dimensions. The Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy was acceptable, .78, and Bartlett’s test of sphericity was significant, p < .001. To ensure reliability, we used Cronbach’s α scores, which were satisfactory for both concerns about the collection and secondary use, α = .88 and α = .81, respectively. We used means of scores to create the two variables: concerns about data collection and concerns about secondary use.

Security concerns. We measured security concerns with an instrument acquired from [5]. The scale included nine items, measuring the level of concerns on a five-point Likert scale, ranging from 1 (very low) to 5 (very high). The scale consisted of three dimensions: authentication, confidentiality, and integrity. To ensure the scale’s validity and reliability, we used PCA. KMO score was satisfactory, .86, and Bartlett’s test of sphericity was significant, p < .001, indicating the suitability of PCA. After specifying the number of factors as three, the factors loaded appropriately. We assessed the reliability of each dimension separately with Cronbach’s α, which was α = .77 for authentication, α = .87 for confidentiality, and α = .89 for integrity. To compute variables, we used the mean of scores for each dimension.

Perceived ability to control. To measure this latent construct, we used the scale developed by [13]. The instrument consists of four items, and the agreement with them is recorded on a Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). To ensure validity and reliability, we use PCA. The KMO and Bartlett’s tests were satisfactory, .73 and p < .001, respectively. The reliability score, measured with Cronbach’s α = .80, was acceptable. To compute the variable, we used means of scores.

Trust. We measured trust with an instrument acquired from [44]. The scale contains five items, and the agreement with items was measured with a Likert scale ranging from 1 (very low) to 5 (very high). The scale consisted of three dimensions: authentication, confidentiality, and integrity. To ensure the instrument’s validity and reliability, we used Cronbach’s α = .80. To compute the variable, we used the mean of scores for each dimension.

4.2 Demographic differences

We used t-test to assess differences in scores of latent and sharing variables. We investigated the differences depending on demographic (male vs. female) and previous experience (privacy or security breaches experienced vs. not experienced). First, we checked for the test assumptions. We did not identify extreme outliers. Although for some variables, there were indicators of deviation from a perfect normal distribution, since t-test is robust to minor deviations from
normality, we decided to conduct the analysis using bootstrapping with the number of samples equaling 1000 and 95% confidence intervals. We examined associations between individual characteristics and latent constructs.

4.2.1 Differences between females and males. We conducted t-test with gender as a grouping factor and latent constructs and sharing preferences. Table 2 presents the means and standard deviations for each variable. There were significant differences between the two outcome variables based on gender. Females scored significantly higher than males in terms of confidentiality concerns, $t(313) = 2.05, p < .05$ (bootstrapped $p = .04$, CI$[-.25, .10]$), Cohen’s $d = .70$. Similarly, they scored significantly higher in integrity concerns, $t(313) = 2.11, p < .05$ (bootstrapped $p = .04$, CI$[-.46, .01]$), Cohen’s $d = .99$. The differences in means between females and males were close to significant levels for the perceived ability to control and trust, where in both cases, females were scoring higher, with single-tailed significance, $t(313) = 1.87, p = .03$ for the ability to control, and $t(313) = 1.74, p = .04$ for trust. However, the bootstrapped sampling did not verify these results.

4.2.2 Differences depending on past experiences. We conducted t-tests to identify whether there are any significant differences in latent constructs and sharing preferences depending on the participants’ previous privacy or security breaches experience. Table 3 presents the means and standard deviations of the variables in question. We found that participants that experienced privacy and security breaches had significantly greater privacy concerns about data collection than participants who did not have such previous experiences, $t(313) = 2.50, p < .01$ (bootstrapped $p = .006$, CI$[.07, .43]$), Cohen’s $d = .78$. Moreover, participants who experienced breaches scored significantly lower in trust than participants who did not have such experiences, $t(313) = 2.67, p < .008$ (bootstrapped $p = .006$, CI$[-.43, -.06]$), Cohen’s $d = .70$. There was a single-tailed significant difference in sharing for personalization, $t(313) = 1.82, p = .03$, indicating that participants who experienced privacy and security breaches were less likely to share. However, the latter finding was not confirmed by bootstrapped sampling.

4.3 Path analysis
Following the APCO framework, we assume the connection between privacy concerns, trust, and behavioral outcomes (sharing) in the present research. To assess the association between the variables studied, we used path modeling, specifically mediation analysis, followed by moderated mediation analysis. We used the perceived ability to control as a covariate in the models. We did not use security concerns because they were strongly correlated with privacy concerns and are semantically similar (see questionnaires in Appendix A.2).

4.3.1 Mediation. We conducted separate mediation analyses with all sharing purposes as outcome variables. In the case of sharing to improve the application, the first path of the model was significant, $R^2 = .24, F(2, 312) = 47.61, p < .001$; here, trust was a significant predictor of privacy concerns, $b = -.23, t(312) = -4.93, p < .001$, and the covariate associated with them significantly ($p < .001$). The second path of the model was also significant, $R^2 = .19, F(3, 311) = 11.58, p < .001$; here, both trust ($b = .03, t(311) = 2.97, p < .05$) and privacy concerns ($b = -.03, t(311) = -3.46, p < .001$) were significant predictors of sharing to improve application. Although the direct path effect was significant ($p < .05, CI95%[.009, .044]$), the bootstrap confidence intervals indicate that partial mediation was also present, CI95%[.003, .013].

In the case of sharing to improve the application’s privacy and security, the first path of the model was significant, $R^2 = .25, F(2, 312) = 47.61, p < .001$; here, trust was a significant predictor of privacy concerns, $b = -.23, t(312) = -4.93, p < .001$, and the covariate associated with them significantly ($p < .001$). The second path of the model was also significant, $R^2 = .38, F(3, 311) = 3.91, p < .05$; here, only privacy concerns ($b = -.02, t(311) = -2.39, p < .05$) were significant predictors of sharing to improve privacy and security. The direct effect of trust on sharing was not significant. However, the bootstrap confidence intervals indicated that partial mediation was present, CI95%[.001, .011].

---

**Table 2: Means and standard deviations of latent constructs and sharing preferences for males and females.**

<table>
<thead>
<tr>
<th>Variable</th>
<th>M</th>
<th>SD</th>
<th>M</th>
<th>SD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection concerns</td>
<td>3.95</td>
<td>.80</td>
<td>4.01</td>
<td>.77</td>
</tr>
<tr>
<td>Secondary use concerns</td>
<td>4.17</td>
<td>.75</td>
<td>4.23</td>
<td>.76</td>
</tr>
<tr>
<td>Authentication concerns</td>
<td>3.44</td>
<td>.79</td>
<td>3.53</td>
<td>.83</td>
</tr>
<tr>
<td>Confidentiality concerns</td>
<td>3.88</td>
<td>.73</td>
<td>4.04</td>
<td>.67</td>
</tr>
<tr>
<td>Integrity concerns</td>
<td>3.25</td>
<td>1.00</td>
<td>3.48</td>
<td>.97</td>
</tr>
<tr>
<td>Ability to control</td>
<td>3.92</td>
<td>.67</td>
<td>4.06</td>
<td>.62</td>
</tr>
<tr>
<td>Trust</td>
<td>2.52</td>
<td>.70</td>
<td>2.66</td>
<td>.70</td>
</tr>
</tbody>
</table>

**Table 3: Means and standard deviations of latent constructs and sharing preferences for people who experienced (EXB) and not experienced (NXB) the privacy or security breaches.**

<table>
<thead>
<tr>
<th>Variable</th>
<th>EXB</th>
<th>M</th>
<th>SD</th>
<th>NXB</th>
<th>M</th>
<th>SD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection concerns</td>
<td>4.17</td>
<td>.64</td>
<td>3.92</td>
<td>.82</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secondary use concerns</td>
<td>4.32</td>
<td>.65</td>
<td>4.16</td>
<td>.78</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication concerns</td>
<td>3.51</td>
<td>.78</td>
<td>3.48</td>
<td>.83</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality concerns</td>
<td>4.02</td>
<td>.70</td>
<td>3.94</td>
<td>.71</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity concerns</td>
<td>3.33</td>
<td>1.00</td>
<td>3.38</td>
<td>.99</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ability to control</td>
<td>4.01</td>
<td>.65</td>
<td>3.98</td>
<td>.65</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trust</td>
<td>2.41</td>
<td>.72</td>
<td>2.65</td>
<td>.70</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sharing for science</td>
<td>.81</td>
<td>.10</td>
<td>.80</td>
<td>.10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sharing for personalization</td>
<td>.78</td>
<td>.09</td>
<td>.78</td>
<td>.10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sharing for privacy &amp; security improvement</td>
<td>.79</td>
<td>.09</td>
<td>.79</td>
<td>.10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sharing for application improvement</td>
<td>.80</td>
<td>.10</td>
<td>.79</td>
<td>.10</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Lastly, in the case of sharing for personalization, the first path of the model was significant, $R^2 = .25$, $F(2, 312) = 47.60, p < .001$; here, trust was a significant predictor of privacy concerns, $b = −.23$, $t(312) = −4.93, p < .001$, and the covariate associated with them significantly ($p < .001$). The second path of the model was also significant, $R^2 = .09, F(3, 311) = 9.24, p < .001$; here, both trust ($b = .03, t(311) = 3.447, p = .001$) and privacy concerns ($b = −.03, t(311) = −2.63, p < .05$) were significant predictors of sharing for personalization. Although the direct path effect was significant ($p = .001, CI95%[.013, .046]$), the bootstrap confidence intervals indicate that partial mediation was also present, $CI95%[.002, .012]$.

4.3.2 Moderated mediation. Using the index of moderated mediation, moderated mediation was identified as an outcome variable for sharing. According to Hayes, the relationship between the indirect effect and the moderator is not zero when bootstrapped confidence intervals of the index of moderated mediation do not include zero, which indicates that the moderated mediation is present [32]. Moreover, there is no need to probe the moderator with statistical tests to assess the significant difference between indirect effects conditioned on different values of the moderator ("any two indirect effects conditioned on different values of [moderator] are statistically different from each other" [32, p. 14]).

We ran moderated mediation analyses, with trust as a predictor ($X$), privacy concerns as a mediator ($M$), and sharing for each of the purposes as an outcome ($Y$). The moderators were demographics and past experiences. To enable easier analysis, instead of investigating each dimension of privacy concerns separately, we created a new variable called privacy concerns based on the mean of all six items. We checked the scale’s reliability, which was satisfactory, Cronbach’s $α = .85$. When running the tests, we did not identify moderating effects of privacy and security breaches. Hence, we removed that variable from the further analysis.

In the model, we investigated whether gender has a moderating effect (interaction) at any of the paths of the model, as presented in Figure 2. The analysis details are presented in Table 4.

In the first path of the model, the only covariate—the ability to control—had a significant effect on privacy concerns, $b = −.44$, $t(310) = 8.22, p < .001$, $CI95%[.33, .55]$. In the second path of the model, trust was a significant predictor of sharing for science ($a_1$), $b = .07, t(308) = 2.49, p < .05$, $CI95%[.01, .12]$. There was a significant interaction effect for privacy concerns and demographics ($c_4' 

\[ b = −.04, t(308) = −2.41, p < .05, CI95%[−.08, −.01]. \]

Particularly, the moderating effects were present for females, with the effect of $−.05, t(308) = −3.20, p < .05, CI95%[−.08, −.02]$. Figure 3 presents the interaction effect. While male participants, regardless of their privacy concerns, score in sharing for scientific purposes similarly, this does not hold among females. The data suggest that, among female participants, there is a decrease in sharing behavior with an increase in privacy concerns.

The bootstrapped index of moderated mediation was significant, confirming the indirect effect of trust on sharing for science when controlling for privacy concerns moderated by gender. The analysis of the conditional effect of the moderator’s focal predictor values indicated a significant change in scores of sharing for science among females, $b = −.05, t(6, 308) = −3.20, p = .002, CI95%[−0.07, −0.02]$. However, this effect does not exist for male participants, $b = −.001, t(6, 308) = −.001, p = .919, CI95%[−0.02, −0.02]$.

5 DISCUSSION

The present research asked questions regarding the relationship between the main components of the APCO macro model: trust, privacy concerns, and behavioral outcome—sharing. Through path modeling, our results confirm that trust significantly affects sharing of health and well-being information and that privacy concerns mediate this relationship. Moreover, we investigated whether previous experiences and gender might have moderating effects on such mediation. Although our results did not indicate significant moderating effects of previous experiences of privacy breaches on sharing, our findings indicate that such experiences affect privacy concerns and trust. Specifically, participants apply their negative experiences with privacy or security breaches, becoming more concerned about who is collecting their information, and less trustful in digital services. Additionally, learning from past experiences seems to affect the willingness to share health and well-being information to receive personalized services and experiences.

The effects of gender among the present study participants seemed to be more significant. First, the results indicate that female
participants are more concerned about information confidentiality and integrity than male participants. Moreover, the findings indicate that females are more trustworthy and have a higher perception of the ability to control their information. More importantly, the results confirm the moderated role of gender in the mediated relationship between trust, privacy concerns, and sharing. However, the difference was visible only in the case of sharing information with third parties for one specific purpose—scientific research. Below we discuss these findings concerning previous theoretical and empirical research and elaborate on potential practical implications.

Before discussing the results, we note that some of the present research findings have small effect sizes. However, the present study results should not be disregarded due to the small effect sizes. Considering the ever-increasing number of people using health and well-being applications (as indicated in Section 1), our results will have more extensive as their implications will affect many more individuals. Similarly, the statistical significance of the results indicates a need for future work that could confirm the present study findings. Additionally, regarding the effect sizes, it is important to note that interpreting complex models with moderating variables and covariates is challenging. Traditional Cohen’s benchmarks might not be suitable since they were based on unrestricted populations [38].

The difficulty of interpretation of effect sizes is also discussed in the context of studies from different psychological sub-disciplines, indicating that the benchmark effect sizes are much larger than the actual effects [59].

5.1 Theoretical discussion

To some extent, our findings confirm the applicability of the APCO macro model in privacy research, contributing to the field of HCI and decision-making studies. Our results indicate a strong relationship between trust, privacy concerns, and information sharing (RQ1). The statistical analyses confirmed either partial (in cases of sharing for science, personalization, and improving application) or full (sharing to improve privacy and security) mediation effects. Although the effect sizes were small, the results indicate that, in the context of sharing health and well-being information with third parties, people might be rational, in an economic sense, about sharing. That is, people’s sharing behaviors relate to their attitudes—people with decreased levels of trust and increased levels of privacy concerns are less likely to share information with third parties. This is an intriguing finding, as it contradicts the privacy paradox (stating that peoples’ privacy concerns mismatch their privacy behaviors) widely discussed in past research. There might be various explanations for the absence of the privacy paradox. It is possible that considering sharing potentially sensitive information, people are more careful and proactive in maintaining their privacy. On the other hand, the absence of the phenomenon might be due to the study design. Unlike in many existing health and well-being applications, in the study, participants were given control and choice over their sharing preferences. Additionally, they were instructed to make changes, which might affect interactions with controls. That said, different prompts or nudges could be added to real-life applications to increase users’ engagement with privacy settings, providing them with usable controls.

Nevertheless, the economic rationality among the study participants differs, considering sharing for science (RQ2). To some extent, the moderating role of gender echoes past work and theoretical assumptions proposed by the sociocultural theory of gender, discussed in Section 2. In our sample, sharing for science behavior among males was at a similar level, regardless of their privacy concerns. One way to interpret this finding is to consider risk and uncertainty research. Assuming that sharing data with third parties is perceived as risky, in agreement with past research, male participants might be more risk-taking and female participants more risk averse, as indicated, e.g., in research about investments, health, or gambling [11, 30]. Another way of interpretation is to consider past research about prosocial behaviors. Our findings imply that male participants share information more willingly than female participants, contrary to stereotypical assumptions that women are more altruistic than men [16]. Therefore, males might be more helpful than females. Such a conclusion agrees with studies from social psychology that showed this is the case, mainly when prosocial behavior happens in a risky situation [25]. The more reasonable and careful approach to sharing information expressed by some of the female participants also reflects past research—e.g., risk aversion among women [17]. This behavior might also be a reflection of females being, in general, more careful in their online interactions because being a woman in an online context might instill vulnerability, particularly when intersected with age, race, and ethnicity [37].
Although, according to the social role theory, females are expected to care more, and sharing health and well-being information could be perceived as altruistic and prosocial, our findings do not entirely correspond with such assumptions. It is possible that among the participants, both males and females have not internalized the traditional agentic and communal gender roles division. Still, it does not imply that the social role theory or the assumptions of the sociocultural theories need to be corrected. To assess the actual effects of gender in the contexts investigated in the present research, one would have to replicate the study in different settings (e.g., different geographical distributions), focusing on different types of sharing that might be considered prosocial—beyond sharing information for scientific research.

5.2 Practical implications

Albeit, at the moment, public and private health providers do not accept user-generated data from personal devices, the digitalization and exchange of data is a topic of interest among policymakers. The EU revised version of Data Governance Act [21] is one example where policymakers recognize how important it is to build an infrastructure allowing sharing of data, including sharing health data with patients, between organizations, and across borders. Similarly, the plans for digital Europe list issues related to health data sharing in their actionable pillars for shaping Europe’s digital future [22]. One pillar is to focus on sharing data for research, diagnosis, and improved health. The second focuses on citizen empowerment and care through digital services, allowing people to take better care of themselves, improve their well-being, and manage healthful living and their health conditions. In the future, these plans might expand beyond health-related data from health providers to data collected by personal devices, which could give better insights into individuals’ health and lifestyles and contribute to scientific research, diagnosis, innovative health solutions, and similar. Here, our findings could be used as they provide insights on sharing attitudes, indicating that people are willing to disclose their sensitive information for the greater good. However, for some people, greater good and prosocial behaviors are not sufficient sharing motivators. To increase sharing of health-related information for research, designers should focus on developing systems that improve trust and diminish privacy concerns. Therefore, the recommendation is to build systems that ensure security and privacy and use solutions that are already perceived as trustworthy. Moreover, our findings could be considered by policymakers, who, when drafting requirements for data-sharing infrastructures, should ensure that such platforms are trustworthy and that users are given control over sharing data with third parties for specific purposes.

According to our data analysis, female participants might share more data for scientific purposes if privacy concerns decrease. Therefore, under specific circumstances, for example, in the case of having privacy indicators, such as transparency of the underlying privacy-preserving data analysis, which can ease people’s privacy concerns, female participants are more likely to share their health and well-being information with a third party (for scientific purposes) and be tricked by privacy theatre than male participants. According to privacy theatre, privacy enhancing technologies (PETs) may provide the “feeling of improved privacy while doing little or nothing to actually improve privacy” [35]. For example, a third party may provide indicators that people rarely read or understand but still give them the impression of safety and security. An indicator or description may emphasize privacy risk reduction without emphasizing the remaining risks and problems. Also, partial transparency may hide important information for decision-making, increasing trust and reducing privacy concerns. People who share their data based on partial information that decreases their privacy concerns may regret their decisions if they learn more about circumstances after making their decisions. Consequently, in all the above scenarios, women would be more likely to share their health and well-being information. They might regret their decision if they learned about the consequences [71]. As for future fair procedures concerning transferring health and well-being data to third parties, policymakers and designers should pay attention to the role of usable and equitable privacy indicators for all that will not negatively affect any specific group.

An intriguing practical implication of the present study is the potential bias in data used for scientific research. This implication is significant for researchers that might have access to and work with user-generated health and well-being data. Considering the identified differences between females and males, one can assume that the existing data sets might be skewed toward males. This unequal distribution might influence scientific research findings, i.e., data sets might contain more extensive richer data sets from males than females. Such biased data sets also impact scientific research findings that rely on AI, which is increasingly deployed in health-related research, e.g., to identify cures for existing diseases. If gender is not accounted for, the research findings based on skewed data sets might be unreliable, misleading, or difficult to generalize. The effects of potential bias in such data sets might be very harmful, considering that health and well-being are at stake. Hence, considering the potential benefits that sharing health-related can bring, it is vital to ensure that all genders are equally represented in such data sets by making them more valuable and usable. Although the algorithmic bias receives more attention in the media and research community, to the best of our knowledge, little research examined the intersection of gender and privacy UI design, which might affect sharing preferences. Our results call for more research on this intersectionality.

5.3 Limitations and future work

The present research has limitations. First, the study was conducted online via Prolific. Thus, there might be self-selection bias among participants, and the participants might be skilled online crowd workers participating in surveys for a living. Therefore, the generalizability of the results might be challenging. However, comparative studies of the different online participants’ pools indicate that Prolific’s participants are more naive than participants from other crowd-sourcing platforms [70].

Moreover, the sample size of the present study is relatively small, and almost half of the participants belong to the younger population, which makes it challenging to generalize about gender differences. However, the study was not purposefully designed to assess gender differences, and the findings surfaced while conducting data analysis. Therefore, although the sample size could have been larger, the
researcher bias is unlikely to be present, enhancing the findings’ reliability. That said, the study should be replicated in the future with a different sample to confirm the current results.

Other demographics, such as age, employment, or education, might affect sharing preferences. However, due to the unequal distribution of participants into different categories of these demographics, we decided not to include them in the statistical analysis. Future research could focus on these demographic characteristics and gather participants in a way that guarantees more balanced distributions.

Considering the limited context of the present research—imagined use of health and well-being application—we recommend partially replicating the study with more specific applications and data types in the future. Similarly, data collection purposes could extend to more than one prosocial behavior, e.g., asking participants to share data for archival and statistical purposes, medical diagnosis and treatment research, pharmacological research, and similar. These could yield different results, which might be used to define context-specific design recommendations.

Similarly, the results might have differed if a different research method had been used. For instance, a field study could identify that behaviors and preferences for sharing differ in real-life scenarios. Unfortunately, the collection of real-life data was not possible for the present research due to the different constraints of the project (e.g., duration, finances). However, different methods enabling the collection of data from real-life behaviors are desirable and recommended to study in the future.

6 CONCLUSIONS

Through an empirical inquiry with 315 participants, the present paper confirms that peoples’ preferences for sharing health and well-being information with third parties strongly rely on trust and privacy concerns. However, the purpose of sharing is not irrelevant. In the context of prosocial behavior, such as sharing for scientific research, factors such as trust and privacy concerns are less influential among males than females. Moreover, the findings indicate that privacy concerns and trust are affected by previous experiences of privacy or security breaches and that females appear to have higher security concerns than males.

These findings contribute to the HCI privacy and decision-making research by confirming some theoretical assumptions from social psychology and behavioral sciences, particularly concerning prosocial behavior, but less concerning social gender roles. Similarly, gender differences may relate to past risk-taking and risk-avoidance research. Additionally, the research findings imply that a privacy paradox does not emerge when people are given control regarding health and well-being data sharing.

Furthermore, policymakers and system designers could apply the theoretical and practical implications of the present study to improve future infrastructures for health and well-being information sharing. Particularly, by considering the factors that affect sharing, such as control over sharing for specific purposes, trust, privacy concerns, and gender dependencies, it might be possible to build more usable technological artifacts that empower citizens to healthier lifestyles.

REFERENCES


A DETAILS OF STUDY DESIGN - QUESTIONS ASKED

In this section, we present the exact questions we asked in different parts of the study including interactive task questions, questions for measuring latent constructs, and demographic questions.

A.1 Interactive task questions

Q1: Select how you would like your data to be processed by third parties:

- I would like to specify where my data should be processed for which purposes.
- I do not care where my data is processed but I want to specify purpose.
- I do not want my data to be processed by any third parties.

If the first option was selected for Q1:

Q1-1: Please specify whether you agree for private companies to process your data, depending on their location:

- I agree that private companies in my country of residence will process my data: Yes, No.
- I agree that private companies outside of my country of residence will process my data: Yes, No.

Q2-1: Please specify whether you agree for governmental organizations to process your data, depending on their location:

- I agree that governmental organizations inside my country of residence will process my data: Yes, No.
- I agree that governmental organizations in countries from the EU and EEA will process my data: Yes, No.
- I agree that governmental organizations in countries outside of the EU and EEA will process my data: Yes, No.

If "Yes" was selected as an answer for either of the questions Q1-1 and Q2-1:

(Purpose question) For which purposes do you allow your data to be processed?

- To improve this application works
- To improve and personalize my experience
- To contribute to scientific research
- To improve the application’s privacy & security

If the second option was selected for Q1: The same purpose question was asked.

A.2 Questions for measuring latent constructs

A.2.1 Privacy concerns. We measured privacy concerns using an instrument acquired from [5]. My level of concern when online companies... (5-point Likert scale from very low to very high):

ask for my personal information is collect too much personal information is gather too much personal information is

My level of concern that online companies may... (5-point Likert scale from very low to very high):

share my personal information without prior authorization is sell my personal information to other companies is misuse my personal information for other reasons without prior authorization is

A.2.2 Security concerns. We measured security concerns with an instrument acquired from [5]. The level of my concern... (5-point Likert scale from very low to very high):

regarding the authenticity of the website I am transacting with is that the website I am transacting with might authenticate someone else mistaking him/her to be myself is

regarding the protection of my personal information from unauthorized access while sending it over the web is

regarding the confidentiality of my personal information while sending it over the web is

regarding the privacy of my personal information while sending it over the web is

The level of my concern... (5-point Likert scale from very low to very high):

regarding the protection of my personal information getting altered while sending it over the web is

regarding the protection of my personal information getting corrupted while sending it over the web is

regarding the integrity of my personal information while sending it over the web is

A.2.3 Trust. We measured trust with an instrument acquired from [44]. Please read the statements below and indicate to what extent you agree or disagree with these statements (5-point Likert scale from Strongly disagree to Strongly agree):

Online companies are trustworthy in handling information about individuals.

Online companies are truthful and fulfill promises related to the information provided to them by me.

I trust that online companies keep my best interests in mind when dealing with information about individuals.

Online companies are in general predictable and consistent regarding the usage of information about individuals.

Online companies are always honest with customers when it comes to using the information that I would provide.

A.2.4 Previous experience of privacy/security breach. Have you had any experiences with privacy or security breaches? E.g., your personal account was hacked, identity misused, personal data leaked?

(Answer options: Yes, Please specify:... No)
A.2.5 Perceived ability to control. To measure this latent construct we used the scale developed by [13]. Please rate the extent to which you agree with the following statements (5-point Likert scale from Strongly disagree to Strongly agree):

- I would only submit accurate and personal information at a website if the site allowed me to control the information I volunteer.
- I would only provide accurate and personal information at a website if the site allowed me to control the information they can use.
- Being able to control the personal information I provide to a website is important to me.
- I would only provide accurate and personal information at a website if their control policy is verified/monitored by a reputable third party.

A.3 Demographic questions

How would you describe your gender? (answer options: Male, Female, Other: (Please self-identify), Prefer not to answer)

How old are you? (Answer options: 18-24 years old, 25-29 years old, […], 60-64 years old, 65 years or older)

Which is the country, you’re currently living in? (Answer options: participants had to type the name of a country)

What is the highest level of education you have completed? (Answer options: High-school, Bachelor’s degree, Secondary school-leaving certificate/Junior High Diploma, General Certificate of Secondary Education (GCSEs), Vocational secondary certification (completion of specialized secondary school/college), Master’s degree or higher, Other school-leaving qualification)

What do you do professionally? (Answer options: University student, Employee/working, Unemployed/seeking employment, Pensioner, Other)