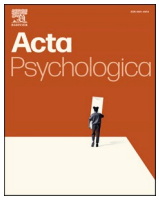
Acta Psychologica 266 (2026) 106746



Contents lists available at ScienceDirect

Acta Psychologica

journal homepage: www.elsevier.com/locate/actpsy





Factors shaping privacy trade-offs in app downloads: The role of privacy ratings, friends' recommendation and resignation among young adults and adults

Jennifer Klütsch [a,*], Annika Kreuder [a,b], Luise Haehn [a], Ida Kuck [a,1], Christian Böffel [a], Ulrich Frick [b], Sabine J. Schlittmeier [a]

[a] Work and Engineering Psychology, RWTH Aachen University, Kackertstraße 9, 52072, Aachen, Germany
[b] HSD Research Center, HSD Hochschule Döpfer, Waidmarkt 3 & 9, 50676, Cologne, Germany

ARTICLE INFO

Keywords:
Privacy decision
App download
Risk-benefit calculation
Young adults
Resignation

ABSTRACT

Mobile apps not only offer numerous benefits but also entail the risk of sharing sensitive data with third parties. This research addresses which factors shape privacy trade-offs among young adults and adults when downloading apps. The investigation involved two experimental vignette studies: In Study 1 ($N = 500$, 79.6% women), we examined young adults, mostly university students, aged 16–29 years to assess if low and high privacy-ratings for apps recommended by friends or a social media platform and offering relevant developmental opportunities affect the probability of downloading them. In Study 2 ($N = 148$, 70.9% women), we examined users aged 18–69 years to assess if low and high privacy-rated apps recommended by friends or found when browsing online, age-related differences, and privacy resignation affect the probability of sharing data with them. In both studies, we found that participants considered privacy ratings when deciding whether to download or share data with an app. While Study 1 found no differences for apps offering relevant developmental opportunities, both studies show a higher reported probability of downloading and sharing data with apps when these were recommended by friends compared to the control conditions (social media platform; browsing). Additionally, Study 2 demonstrated that participants under 29 years of age and with higher levels of resignation exhibited a higher probability of sharing data. These findings highlight that privacy ratings can support privacy decisions at the app download stage, but also emphasize the need for future interventions, especially for younger and resigned users.

1. Introduction

Mobile apps provide users with a wide range of benefits, from messenger apps facilitating seamless communication to cooking apps providing healthy recipes. However, this convenience can come with inherent privacy risks, where users "pay" these services and third-party providers with personal data (Buck et al., 2014; Wottrich et al., 2018). The initial app download stage is a critical point for protecting against privacy-invasive apps as sensitive data such as phone numbers can be transferred without interacting with the app (Harborth & Pape, 2021; Kollnig et al., 2022). Despite these risks, the global number of app downloads has surged from about 141 billion in 2016 to 257 billion in 2023 (TechCrunch, 2024). This trend particularly concerns younger users who download apps more frequently compared to older users (Appfigures, 2022) and are more inclined to disclose personal data on social media (Kezer et al., 2016). To identify which factors shape privacy trade-offs among users, particularly younger users, we explore how they choose to download and share data with apps. This investigation included two experimental vignette studies. In Study 1 ($N = 500$, 79.6% women), we examined the privacy trade-offs of young adults aged 16–29 years in more detail. We assessed if low and high privacy-rated apps recommended by friends or a social media platform and offering relevant developmental opportunities, such as entering professional life, affect young adults' probability of downloading them. In Study 2 ($N =$

* Corresponding author.
E-mail addresses: kluetsch@psych.rwth-aachen.de (J. Klütsch), annika.kreuder@psych.rwth-aachen.de (A. Kreuder), luise.haehn@psych.rwth-aachen.de (L. Haehn), ida.kuck@ika.rwth-aachen.de (I. Kuck), christian.boeffel@psych.rwth-aachen.de (C. Böffel), sabine.schlittmeier@psych.rwth-aachen.de (S.J. Schlittmeier).
[1] Institute for Automotive Engineering, RWTH Aachen University, Steinbachstraße 7, 52074 Aachen, Germany.

https://doi.org/10.1016/j.actpsy.2026.106746
Received 4 June 2025; Received in revised form 13 March 2026; Accepted 25 March 2026
Available online 7 April 2026
0001-6918/© 2026 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

148, 70.9% women), we investigate how age-related differences and differences in privacy resignation affect the likelihood of sharing data with low and high-privacy rated apps that are recommended by friends or found while browsing online. Study 2 extends the empirical insights on young adults to a broader age group and systematically examines how resignation, found prevalent in young adults, influences online privacy decisions at the app download stage.

1.1. Risk-benefit calculation under uncertainty

These type of privacy decisions are related to one's *informational privacy* (Masur, 2018; Trepte & Masur, 2023), defined as control over "when, how, and to what extent information about [oneself] is communicated to others" (Westin, 1967, p. 5). Legal frameworks such as the General Data Protection Regulation (GDPR) define several lawful bases for processing personal data (e.g., consent, performance of a contract or legal compliance). When privacy decisions are based on consent, the GDPR requires such consent to be informed and unambiguous (General Data Protection Regulation, 2016). Even though the *privacy calculus* emphasizes that users should be able to rationally weigh up the perceived benefits against the associated privacy risks, research shows that users often engage in rather paradoxical privacy behavior that does not align with their initial privacy concerns. This phenomenon is known as the *privacy paradox* (Kokolakis, 2017; Norberg et al., 2007). Privacy research highlights several reasons why users face difficulties engaging in rational risk-benefit calculations. One reason is that users decide to share personal data based on *incomplete information* (Acquisti, 2004; Acquisti et al., 2017; Barth & de Jong, 2017). This may occur because privacy information is not presented visibly enough during app downloads (Barth et al., 2019; Gu et al., 2017) or combined with deceptive design patterns, such as defaults (Bösch et al., 2016). In addition, users often have limited time or mental resources to process all information related to certain risks and benefits (*bounded rationality;* Simon, 1955) and make privacy decisions under high uncertainty (Acquisti, 2004; Acquisti et al., 2017; Barth & de Jong, 2017). As a consequence, users are influenced by cognitive biases and heuristics affecting their risk-benefit assessment (Acquisti et al., 2017; Barth & de Jong, 2017; Kokolakis, 2017, see Fig. 1).

User studies support the influence of heuristics (e.g., *take-the-best heuristic*; Dogruel et al., 2015) and biases (e.g., *present bias*; Lünich et al., 2021) in privacy decision-making: For example, Lünich et al. (2021) found that users often overestimate immediate benefits, with nearer benefits increasing the perceived app benefit in contexts like online shopping, political engagement and self-tracking (*present bias;* see also Acquisti et al., 2020). Other researchers found similar privacy trade-offs during app download decisions, where initial privacy concerns were outweighed by immediate benefits of an app, such as its value or functionality (Barth et al., 2019; Wottrich et al., 2018).

In addition, social cues and norms seem highly important for users' privacy decisions. Social theory-based interpretations assume that users might engage in paradoxical privacy behavior to maintain their connections with others (Kokolakis, 2017). Several user studies support this assumption: For example, researchers have demonstrated that social norms affect users' self-disclosure, both offline (Mehdy et al., 2021) and on social media (Masur et al., 2021, 2023). Similar effects were found during app downloads where social cues such as the apps' popularity (Gu et al., 2017; Harborth & Pape, 2021), reviews (Barth et al., 2019; Dogruel et al., 2015) or the usage behavior of others (Kroschke & Steiner, 2017) were found to increase the intention to download or use the app. This tendency to imitate the behavior of relevant others and their drive to share information is also known as *herding* in related literature (Acquisti et al., 2020).

Another explanation for users' paradoxical privacy behavior is *privacy cynicism*, described as an "attitude of uncertainty, powerlessness and mistrust towards handling of personal data by online services, rendering privacy protection behavior subjectively futile" (Hoffmann et al., 2016, p. 5). Accordingly, this attitude can invoke resignation in privacy protection online. *Privacy cynicism* is described as a coping mechanism that reduces cognitive dissonance for users who are concerned about protecting their privacy but feel unable to do so effectively (Hoffmann et al., 2016). It is closely related to *digital resignation*, which is defined as a "condition produced when people desire to control the information digital entities have about them but feel unable to do so" (Draper & Turow, 2019, p. 1). Related literature differentiates further concepts of this resigned attitude towards online privacy threats (e.g., *privacy fatigue*). Although these concepts are related, their terminology and applied empirical approaches are distinct (see Draper et al., 2024, for an overview). Our study draws on the concept of *privacy cynicism*, as defined by Hoffmann et al. (2016) and focuses on the resignation facet measured with the questionnaire by Lutz et al. (2020), which captures four sub-facets: mistrust, powerlessness, uncertainty, and resignation. User studies confirm that *privacy cynicism* reduces online privacy protection: Although privacy cynics have moderately high levels of privacy concerns, they were found to engage in low levels of privacy protection behavior (Schomakers et al., 2019). In this regard, feelings of resignation in particular appear to reduce the role of privacy risks for users' intention to disclose (Wirth et al., 2018) and prevent users from acting in line with their privacy concerns (Lutz et al., 2020). In a large-scale online study, Lutz et al. (2020) examined the different facets and outcomes of *privacy cynicism* and found that resignation univocally reduced privacy protection on websites. Yet, more research is needed to understand how resignation affect privacy protection in different contexts and situations (e.g., during app downloads) and which antecedents contribute to resignation online (Lutz et al., 2020). In addition, future research is

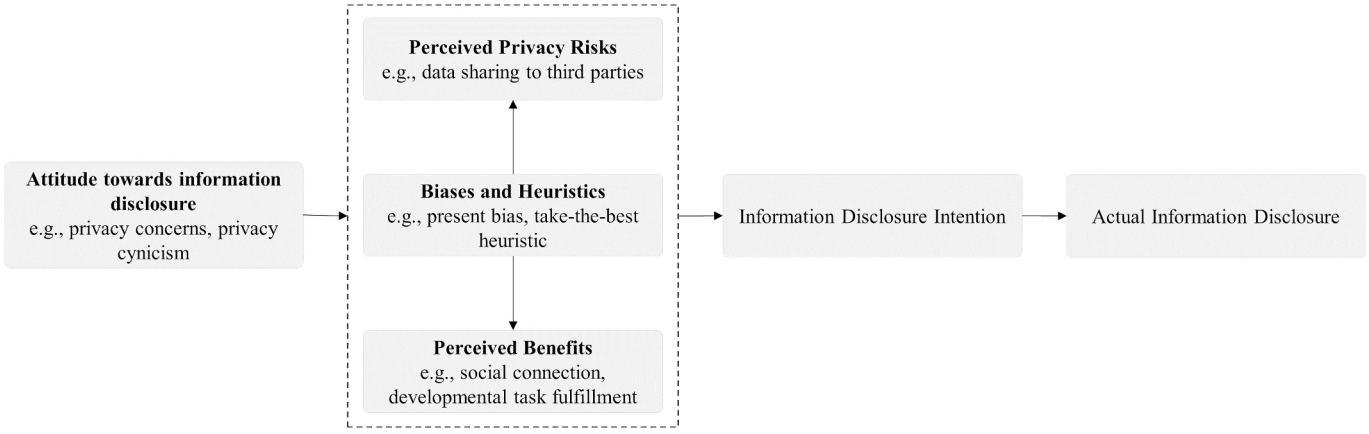


Fig. 1. Theoretical framework of users' biased risk-benefit calculation (based on Barth & de Jong, 2017).

needed to expand upon cross-sectional data insights through longitudinal and experimental studies (van Ooijen et al., 2024).

1.2. Young adults as vulnerable user group

Young adults (approx. 18 to 29 years, Sawyer et al., 2018) seem of particular interest to future research in this regard. On the one hand, user studies have found exploratory effects that younger users experience higher degrees of privacy cynicism (Schomakers et al., 2019; van Ooijen et al., 2024). On the other hand, they seem more influenced by their peer group (Kezer et al., 2016; Kreuder et al., 2023; van den Broeck et al., 2015). For instance, van den Broeck et al. (2015) found that young adults tend to share more personal information to a wider audience to fulfill their increased need of self-presentation. Additionally, research suggests that this user group experience higher levels of Fear of Missing Out (FoMO) (Przybylski et al., 2013). This urge to join in is known to increase privacy and security risks by heightened data sharing on social media (van der Schyff & Flowerday, 2023), along with riskier online behavior such as password sharing (Popovac & Hadlington, 2020) and susceptibility to phishing (Klütsch, Schwab, et al., 2024).

From a developmental perspective, young adults engage in riskier online behavior due to their striving towards developmental tasks, such as entering professional life (Havighurst, 1948; Seiffge-Krenke, 2015; Steijn & Vedder, 2015). A developmental task occurs at a particular life stage and, if successfully completed, contributes significantly to an individual's happiness and future success (Havighurst, 1948). Researchers argue that online services can provide adolescents and young adults with opportunities tailored to a relevant developmental task, influencing their online security and privacy behavior (Klütsch et al., 2025; Peter & Valkenburg, 2011; Steijn & Vedder, 2015). For example, messages inviting young adults to an upcoming event and offering the opportunity to belong to their peer group (compared to other developmental opportunities) have been found to lead to an increased susceptibility to phishing (Klütsch et al., 2025). Similarly, in privacy research, Steijn (2014) has found that young adults, like adolescents, seem to post more frequently on social media in order to belong to their peer group and, in contrast to other age groups, actively manage their privacy settings as they transition into professional life. When integrating theoretical perspectives on privacy research (e.g., Barth & de Jong, 2017), this usage behavior can be explained by a developmentally driven overestimation of certain online functionalities that alter young adults' risk-benefit calculations: When functional opportunities offered by digital services or apps align with relevant developmental tasks (e.g., entering professional life), they can be perceived as highly beneficial to young adults. Such developmental benefits could then encourage young adults to engage in privacy trade-offs despite their initial privacy concerns. Given young adults' increased developmental need to belong to a peer group, the same applies to apps or services recommended by friends, which can be perceived as increasingly beneficial. Research on developmental and psychosocial factors (e.g., social influence) among adolescents and young adults however remains limited in various areas of digital competence, including privacy behavior (Kreuder et al., 2024). While previous research has identified age-related differences in privacy behavior between younger and older users (Kezer et al., 2016; Steijn, 2014; van den Broeck et al., 2015), there is still a lack of studies that directly assess the role of developmental tasks (Steijn, 2014). This underscores the need for more research to systematically examine how developmental and/or social benefits encourage privacy trade-offs online.

1.3. Risk assessment through privacy indicators

Social and developmental influences could be accentuated at the app download stage, as privacy information is often not visible to the user and hidden behind scrolling (Barth et al., 2019; Gu et al., 2017). Privacy indicators have been discussed as a promising intervention by providing users with easily understandable risk information, for example, in form of automated visualizations (Garcia et al., 2025; Harkous et al., 2018; Zaeem et al., 2018) or as contextual information related to the context of use (Windl et al., 2022).

Visualized privacy indicators can be defined as a type of nudge that direct users' attention and their automatic system including cognitive heuristics and biases, to promote a certain choice or behavior (Caraban et al., 2019; Hansen & Jespersen, 2013; Thaler & Sunstein, 2009). Several researchers have tested the privacy-enhancing effect of these indicators. Studies show that privacy indicators, such as colored rankings with specified risk information, can increase user trust in digital services by clarifying data collection practices (Barth et al., 2021) as well as reduce data disclosure (Hughes-Roberts, 2015). These findings are supplemented by Garcia et al. (2025), who developed an LLM-based browser extension. The researchers demonstrated that low privacy ratings increased perceived privacy risks and reduced perceived benefits of using a certain website (Garcia et al., 2025). Similar effects were shown by Meier and Krämer (2024). Although privacy indicators could not negate the importance of immediate benefits, they made privacy risks more apparent to users, including those who felt resigned to protecting their data (Meier & Krämer, 2024). At the app download stage, similar effects were found. For example, it was found that a label bar can encourage the choice of less privacy-invasive apps (Bock & Momen, 2020). In addition, evidence is found that simple privacy indicators, such as locks or colored privacy meters, can influence the decision to choose a particular app (Stöver et al., 2021). Incorporating a privacy indicator into our experimental design could support the investigation of social influence and developmental opportunities in low- and high-rated privacy decisions and provide insights into the role of resignation in these decisions.

1.4. Our present research

To identify how these factors influence privacy trade-offs, we explore how users, especially young adults, choose to download and share data with apps that compromise their privacy in two studies. Based on previous theoretical work (see Fig. 1), we first aim to systematically investigate how young adults weigh social (e.g., connecting with friends) and developmental benefits (e.g., entering professional life) against privacy risks at the app download stage. In Study 1, we provide a novel developmental perspective that shows empirical insight on how friends' recommendation and relevant developmental opportunities offered by different categories of apps influence young adults' app downloads for low and high privacy rated apps. With our research, we aim to extend the limited understanding of developmental and psychosocial factors (Kreuder et al., 2024; Steijn, 2014). In a second step, we aim to examine whether social drivers, found highly impactful in Study 1, extend beyond the age group of young adults, while additionally testing the role of privacy resignation among young adults and adults. Our study provides a deeper understanding of privacy cynicism and resignation beyond cross-sectional data of previous studies (e.g., van Ooijen et al., 2024) and offers empirical insights from experimental online vignette studies.

While privacy indicators are often cited as a practical tool to help users to make more informed privacy decisions, we experimentally vary the risks associated with downloading an app through a simple privacy indicator. In contrast to previous studies (Gu et al., 2017; Harborth & Pape, 2021; Wottrich et al., 2018), this allow us to determine how simple privacy indicators guide users' privacy decisions and to investigate the role of social influences and developmental opportunities in their privacy trade-offs. We built upon similar work of Meier and Krämer (2024), who adopt privacy scores as situational risk cue to investigate the intrapersonal privacy trade-offs users engage in.

Based on previous privacy literature, we assume that users, particularly younger users, value friend's recommendation and relevant developmental opportunities as immediate benefits of an app that may

outweigh the long-term privacy risks (*present bias*; Acquisti et al., 2020; Lünich et al., 2021). This assumption is built on the theoretical work on developmental tasks highlighting that young adults strive to complete certain tasks such as belonging to their peer group or entering professional life (Havighurst, 1948). In addition, we expect that friend's recommendation increase the download and data sharing with an app through users' tendency to imitate the behavior of relevant others (Acquisti et al., 2020). Because previous research emphasized reduced privacy protection behavior among users with higher resignation (Lutz et al., 2020), we assume similar effects in our research. Fig. 2 illustrates the research questions and key assumptions.

2. Study 1

Study 1 examines how recommendations and relevant developmental opportunities offered by different app categories influence young adults' app downloads under low and high privacy ratings. Given that simple privacy indicators should make privacy risks more salient to the user (Bock & Momen, 2020; Garcia et al., 2025; Meier & Krämer, 2024), we propose that high (vs. low) privacy ratings increase users' probability of downloading an app (*Hypothesis 1*).

However, research also highlights that users' privacy decisions are often influenced by social cues such as the app's popularity (Gu et al., 2017; Harborth & Pape, 2021), reviews (Barth et al., 2019; Dogruel et al., 2015) or the usage behavior of others (Kroschke & Steiner, 2017). As outlined in previous work, connecting with one's peer group by following their recommendation could thus be valued as an immediate social benefit that may outweigh the abstract, often long-term privacy risks displayed by the privacy score in our study (Acquisti et al., 2020; Lünich et al., 2021). Conversely, this could increase users' probability of downloading the app, irrespective of the perceived privacy risks and could apply in particular to young adults, who face the developmental need of belonging to their peer group (Havighurst, 1948; Seiffge-Krenke, 2015). We propose that a friend's recommendation increases the probability of downloading compared to a social media platform recommendation, for both high and low privacy rated apps (*Hypothesis 2*).

Aside from connecting with their peers, young adults face several other developmental tasks, such as being in a relationship or entering professional life (Havighurst, 1948; Seiffge-Krenke, 2015). These tasks may also provide important benefits. For example, job apps could help prepare them for professional life. Like social benefits, this could be seen as an immediate and important developmental benefit that may outweigh long-term privacy risks. We therefore propose that apps aligned with unfulfilled and/or important developmental tasks increase the probability of downloading compared to apps aligned with fulfilled or unimportant tasks, for both high and low privacy rated apps (*Hypothesis 3*).

Finally, we explored differences in the download probability across the four categories of apps that offer different developmental opportunities and individual predictors, including age-related differences in young adults and gender.

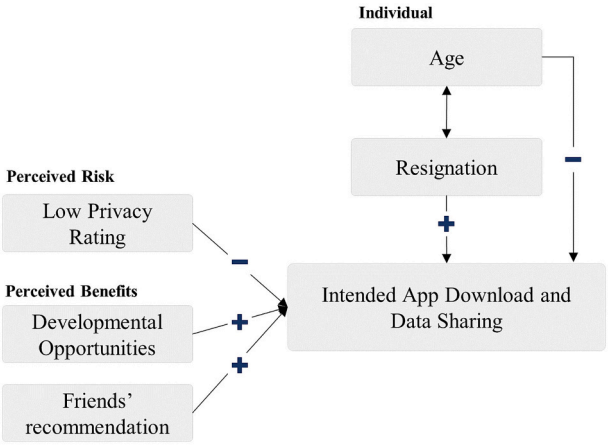


Fig. 2. Overview of the research questions and key assumptions tested in Study 1 and Study 2.

2.1. Method

We conducted an online experimental vignette study with 500 young adults aged 16 to 29 years ($M = 22.28$ years, $SD = 2.56$). We included participants between 16 and 29 years to capture the transition from late adolescence to young adulthood. This age range aligns with previous literature, which defines young adulthood as up to 29 years old (Sawyer et al., 2018). Vignettes refer to short, carefully constructed, text- and image-based descriptions, in our case, of app download scenarios (Atzmüller & Steiner, 2010). The app download scenarios contained text-based recommendations by a social media platform or friend group (*recommendation*, within-subject). Apps were presented in image-based app store depictions and with low or high privacy ratings (*privacy rating*, within-subject). Participants received four apps from one out of four app categories (*app category*, between-subject) that offer different developmental opportunities. The developmental opportunities were selected to fulfill developmental tasks, discussed as relevant to young adults both in theoretical work on the concept of developmental tasks (Havighurst, 1948) and in related privacy research (Borca et al., 2015; Coyne et al., 2013; Steijn, 2014; van den Broeck et al., 2015). This resulted in the following app categories: (1) dating apps for forming a committed relationship, (2) job apps for entering professional life, (3) messenger apps for belonging to one's peer group and (4) self-discovery apps for developing one's hobbies and interests. After each app scenario, we asked how likely participants were to download an app in the different app download scenarios on a scale from 0% to 100% as the dependent variable (DV). The study was conducted as part of a larger research project A-DigiKomp with other studies on different areas of digital competence.

2.1.1. Participants

553 participants were recruited via email, social media or direct inquiries to schools and universities. All participants provided informed consent and were able to win vouchers (1 × 100€, 2 × 50€, 5 × 25€, 15 × 15€) for their participation. Participation was voluntary and students from three universities received course credits for participation. Due to our focus on young adults aged between 16 and 29 years, participants older than 29 years and those who failed control items were excluded ($N_{excluded} = 53$).

The final sample consisted of 500 young adults (398 women, 99 men, 3 with no indication; $M = 22.3$ years, $SD = 2.6$). The majority of participants indicated A-Levels (67.8%) as their highest educational degree and were university students (80%). This was followed by apprentices (7.8%) or employees (7.8%). Furthermore, the majority of participants reported using WhatsApp (97.8%), Instagram (86.8%) and/or YouTube (81.2%).

2.1.1.1. Ethics and informed consent. Study 1 was approved by the ethical committee of HSD Hochschule Döpfer (BEth_20_22, decision of May 19, 2022) with no ethical concerns raised. All participants provided informed consent prior to participation. Participants agreed to the privacy protection regulation and their anonymized and aggregated data being stored and published in a data repository. Due to the high standard of privacy protection applied, none of their data was identifiable after collection. Participation was voluntary, and participants retained the right to withdraw at any time.

2.1.1.2. Power analysis. We conducted an a-priori power analysis based on Arend and Schäfer (2019) using the *simr* package in RStudio (RStudio

Team, 2022) to estimate the required sample size. For our mixed-subject design, we assumed a medium Level 1, Level 2 direct effects and a cross-level interaction effect of 0.30 under a medium intraclass correlation coefficient (ICC) of 0.30. The analysis indicated a minimum of 382 participants to achieve a power greater than 0.80 for all effects. We maximized the sample size within the study period to increase the informational value of our study.

2.1.2. Procedure

The procedure of Study 1 is visualized in Fig. 3. After the welcoming and informed consent, participants were queried about their socio-demographic information (e.g., age, gender) and their internet, social media and instant messaging app use. Throughout the study, participants received four text- and image-based vignette scenarios about their app download behavior (see Section 2.1.3). In the vignette scenarios, participants indicated their probability to download each app on a scale from 0% to 100%. After completion of all vignette scenarios, follow-up questionnaires were queried (see Section 2.1.4). In the debriefing, participants received detailed information on the study aim. The whole study took approximately 30 to 40 min and was hosted by Pavlovia (https://pavlovia.org/) using PsychoPy (Peirce et al., 2019), HTML and JavaScript.

2.1.3. Vignette scenarios

Participants received four apps of one app category (see Fig. 3) with text-based scenarios and image-based app store screens. Two apps were recommended by friends and two recommended by a social media platform in text-based scenarios (see Table 1), with one app of each recommendation type assigned a low privacy rating and one app of each recommendation type assigned a high privacy rating. The fictional app store depicted the privacy rating with a simple privacy lock indicator that showed one lock for low privacy and five locks for high privacy. To avoid social desirability bias and approximate real-world app store environment, we did not include further briefing on the privacy indicator and built upon research from Stöver et al. (2021), who found similar privacy indicators as generally intuitive and interpretable. Both the text-based scenario and the image-based app depiction (see Fig. 4, "About this app") addressed how the app could support the fulfillment of developmental tasks. The app designs in each app category were counterbalanced for privacy rating and recommendation and were balanced in color to avoid systematic effects of app design (see Fig. 4). In addition, the app store depiction was designed to closely resemble real app store screenshots. For each app scenario, we asked participants about their probability of downloading the app on a scale from 0% to 100%.

Table 1
Translated text-based scenario for social media platform and friends' recommendation to each app category and developmental opportunity.

Recommendation	Short-text scenario
Social media platform	You are reading through your Instagram feed. Based on your interests, you receive a recommendation in the posts for the new [app category] app [app name] – which is supposed to show you the perfect matches and help you find your next date. [being in a relationship] vs. – which is designed to help you find a job. [entering professional life] vs. – for easy messaging and quick video chats with your friends. [belonging to one's peer-group] vs. – which is designed to help you get to know yourself better and discover new hobbies. [developing one's hobbies and interests]
Friend	At a get-together, your friends tell you that they can recommend the new [app category] app [app name]. – They think the new matches are perfect for them and are looking forward to the next date. [being in a relationship] vs. – The app helped them greatly in their search for their first job. [entering professional life] vs. – The simple exchange of messages and quick video chats have convinced them to use the messenger app regularly. [belonging to one's peer-group] vs. – They tell you that they have gotten to know themselves better and discovered new hobbies. [developing one's hobbies and interests] Later, a friend sends you the link to the app.

2.1.4. Follow-up questionnaires

Table 2 provides an overview of the items analyzed in this study. We administered an extended 13-item version of the developmental task questionnaire for young adults by Seiffge-Krenke (2001) (see DTQ-YA-2 for full item list; Seiffge-Krenke et al., 2025). Our study focused on the fulfillment and importance of four developmental tasks addressed by different app categories and measured through the items on (1) forming

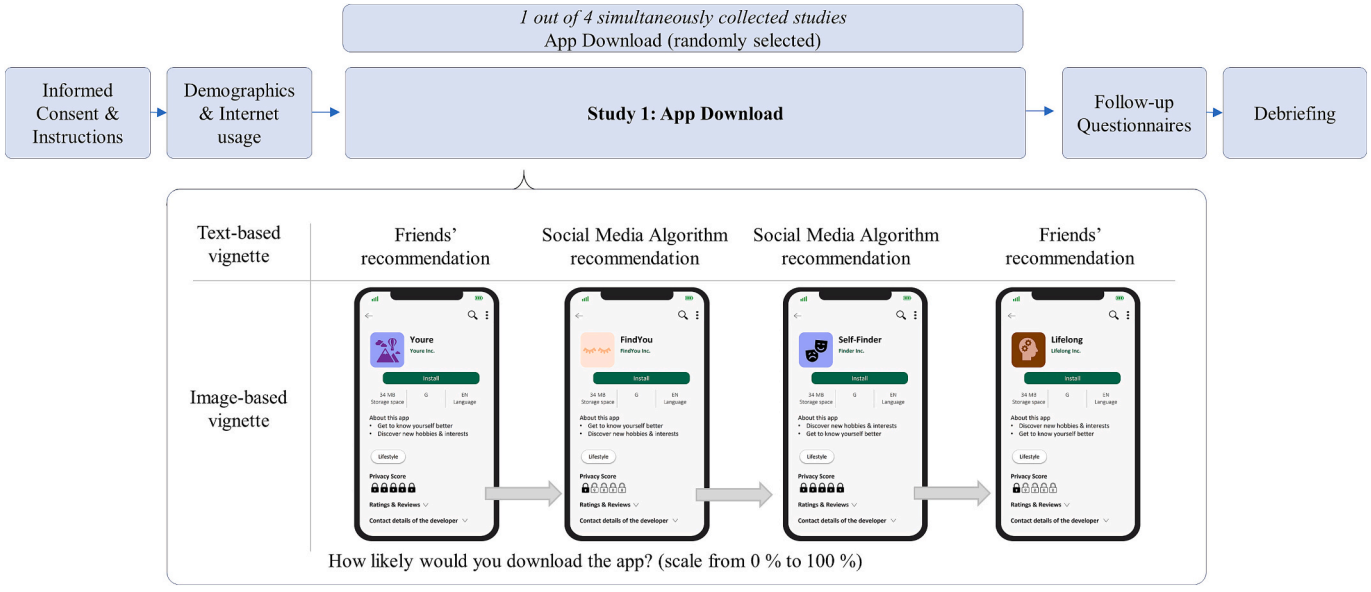


Fig. 3. Overview of the procedure of study 1 for the translated app category self-discovery app as an example.
Note. The app designs in Study 1 were counterbalanced for privacy rating and recommendation to avoid systematic effects of app design.

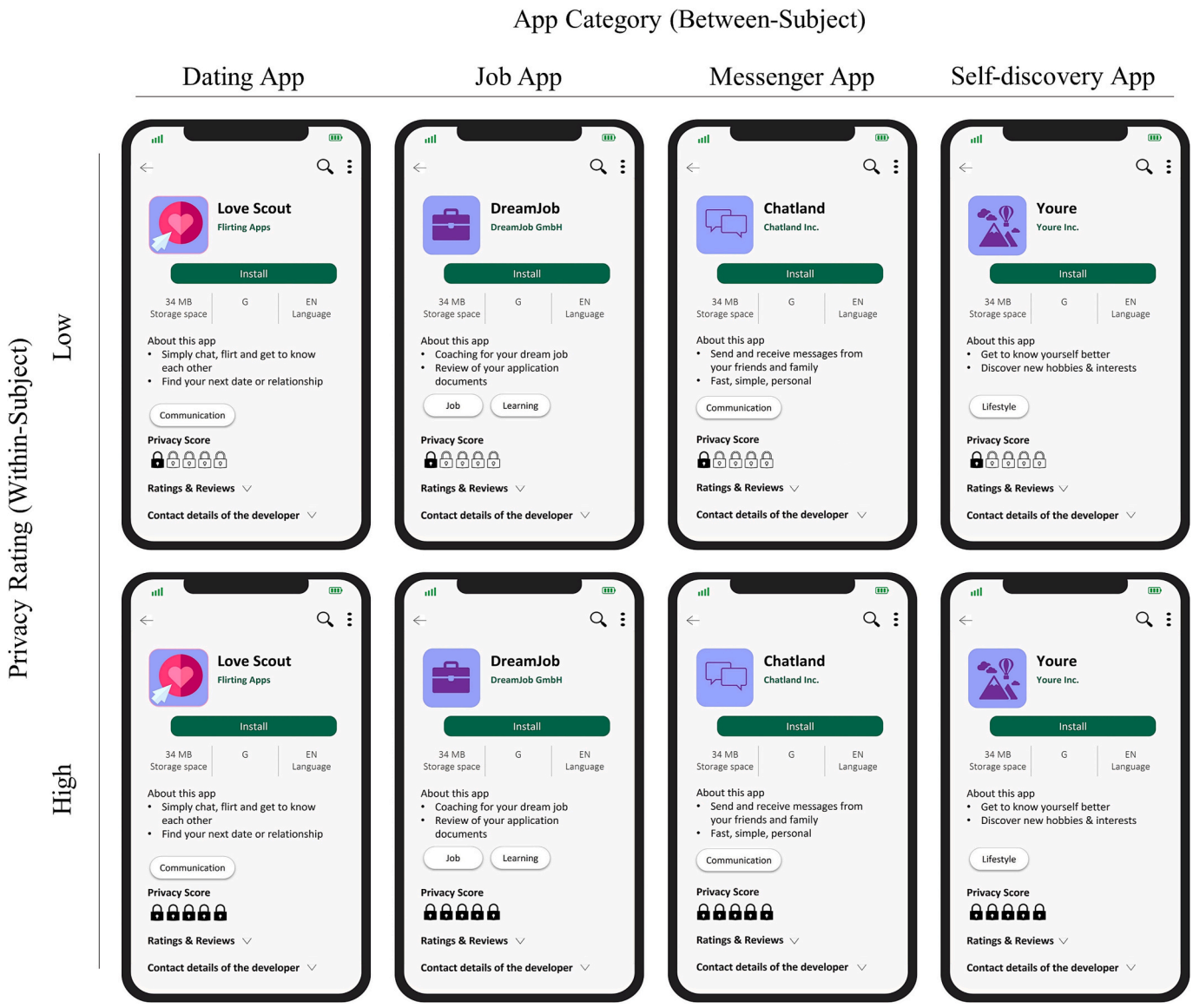


Fig. 4. Translated examples of the image-based app store depictions for dating apps, job apps, messenger apps and self-discovery apps and low as well as high privacy ratings.

Note. Participants received four apps with counterbalanced app designs of one out of four app categories to avoid carryover effects and systematic effects of app design. This figure shows one app design per app category.

Table 2
Items on developmental task fulfillment and importance and control items.

Measures	Descriptions	Characteristics	Sources
Adapted items of the DTQ-YA	Developmental task fulfillment 3-point scale with three response options: (1) "I have not reached yet", (2) "I have started", (3) "I have already reached" – Have you already started your professional life? – Are you currently in a steady relationship? – Have you already developed interests/hobbies that you are passionate about? – Are you part of a circle of friends or a social group that suits you?	Hypothesized predictor coded as either not fulfilled (0) or fulfilled (1)	Translated and adapted from Seiffge-Krenke (2001) (see DTQ-YA-2 for full item list; Seiffge-Krenke et al., 2025)
	Developmental task importance 3-point scale with three response options: (1) "not important", (2) "somewhat important", (3) "very important" – Do you wish to enter working life? – Do you want a steady relationship? – Do you wish to develop interests/hobbies that you are passionate about? – Do you wish to become part of a circle of friends or a social group that suits you?	Hypothesized predictor coded as either not important (0) or important (1)	
Control items	6-point Likert scale ranging from 1 "I do not agree at all" to 6 "I strongly agree" – To make sure you are fully on board, please select "strongly agree" here. 3-point scale with three response options: (1) "not important", (2) "somewhat important", (3) "very important" – To make sure you are fully engaged, please select "not important" here.	Control item Participants who failed the control items were excluded	

a committed relationship, (2) entering professional life, (3) belonging to one's peer group and (4) developing one's hobbies and interests of both scales. Participants rated fulfillment of the developmental tasks by selecting "I have not reached yet," "I have started," or "I have already reached", and importance by selecting "not important at all", "somewhat important" and "very important". Tasks were classified as not fulfilled (0) if participants selected "not reached yet" and as fulfilled (1) if they selected "started" or "already reached". Developmental tasks were categorized as not important (0) if participants rated them as "not important at all" and as important (1) if participants rated the associated item as "somewhat important" or "very important". As a result, 70.2% of participants rated the developmental task addressed by the app presented to them as fulfilled, and 93.2% rated it as important. Two control items were incorporated to ensure attentive participation (see Table 2). Moreover, questions on sociodemographic details and internet usage (duration of internet use, type of messengers and social media used) were administered for our study.

2.2. Results

The statistical software RStudio (RStudio Team, 2022) was used for analysis. Given the repeated measures design and an intra-class coefficient (ICC) indicating that 19.9% of the variance in *download probability* was explained by between subject differences, a multilevel structure was necessary. We ran multilevel linear regression for *download probability* using the lme4 package (Bates et al., 2024). All predictors (except for age) were dummy coded as dichotomized variables, with age being grand-mean centered. Significance was tested at $\alpha = 0.05$.

The experimental variables *privacy rating* (low vs. high), *recommendation* (social media platform vs. friends) and *app category* (dating app, job app, self-discovery app vs. messenger app), including their interaction effects, were added to the final multilevel regression analysis. In addition, the hypothesized predictors *developmental fulfillment* and *importance* were added as single predictors to the final multilevel regression analysis. Finally, exploratory predictors (*age*, *gender*) were tested to determine if they improved the model fit. *Age* did not significantly improve model fit ($p = .08$) and was therefore not added to the final multilevel regression analysis, whereas *gender* significantly improved model fit and was included ($p = .01$).

2.2.1. Final multilevel linear regression

The final multilevel linear regression contained the following predictors: *recommendation* (social media platform vs. friend), *privacy rating* (low vs. high) and *app category* (dating app, job app, self-discovery app vs. messenger app), along with their interaction effects as well as *developmental fulfillment* (not fulfilled vs. fulfilled), *developmental importance* (not important vs. important) and *gender* (women vs. men). Table 3 summarizes the results of the final multilevel linear regression. Additional results from the final regression analysis with different reference categories of the predictor *app category* can be found in the Appendix A.1.

In line with *hypothesis 1*, the analysis revealed the proposed effect of *privacy rating* (see Fig. 5): Apps with high privacy ratings were more likely to be downloaded than apps with low privacy ratings ($b = 28.41$, 95% CI: [23.36, 33.47], $p < .001$). In addition, the proposed effect of *recommendation* was found (*hypothesis 2*): When apps were recommended by friends, participants indicated a higher download probability than when apps were recommended by a social media platform ($b = 12.53$, 95% CI: [7.47, 17.59], $p < .001$, see Fig. 5). An interaction effect between *recommendation* and *privacy rating* was also found ($b = 10.41$, 95% CI: [3.26, 17.56], $p = .005$). In line with Sommet and Morselli (2021), we explored this interaction by splitting the data by *privacy rating* and computed two multilevel linear regression analyses on the split data sets. The split data analysis showed that the effect of *recommendation* was confirmed for high and low privacy ratings, but was stronger for high privacy ratings ($b = 22.94$, 95% CI: [18.92, 26.97], $p < .001$) compared to low privacy ratings ($b = 12.53$, 95% CI: [8.88, 16.18], $p < .001$).

Contrary to our *hypothesis 3*, we found no effect of *developmental task fulfillment* ($b = 2.11$, 95% CI: [−2.19, 6.41], $p = .34$) or *developmental task importance* ($b = -0.13$, 95% CI: [−7.27, 7.02], $p = .97$) on download probability. In other words, apps addressing unfulfilled and/or important developmental tasks did not increase participants' probability of downloading compared to apps addressing fulfilled or unimportant

Table 3
Results of the final multilevel linear regression for download probability (DV) predicted by recommendation (social media platform vs. friend), privacy rating (low vs. high), app category (self-discovery, job, dating vs. messenger) and their interaction terms as well as developmental fulfillment (not fulfilled vs. fulfilled), importance (not important vs. important) and gender (women vs. men).

Predictors	Coeff. (*b*)	*t*-value	p	95% CI
(Intercept)	0.34	0.07	0.945	−9.19 to 9.86
Friends' recommendation[a]	12.53	4.84	< 0.001***	7.47 to 17.59
High privacy rating[b]	28.41	10.98	<0.001***	23.36 to 33.47
Self-discovery app[c]	9.36	2.68	0.007**	2.56 to 16.16
Job app[c]	7.56	2.12	0.034*	0.60 to 14.52
Dating app[c]	4.29	1.23	0.217	−2.48 to 11.06
Gender	5.63	2.47	0.014*	1.19 to 10.07
Developmental task fulfillment	2.11	0.96	0.340	−2.19 to 6.41
Development task importance	−0.13	−0.04	0.972	−7.27 to 7.02
Friends' recommendation[a] * Self-discovery app[c]	0.66	0.17	0.863	−6.82 to 8.15
Friends' recommendation[a] * Job app[c]	−2.69	−0.71	0.478	−10.09 to 4.71
Friends' recommendation[a] * Dating app[c]	−3.22	−0.87	0.384	−10.44 to 4.00
High privacy rating[b] * Self-discovery app[c]	0.36	0.09	0.925	−7.13 to 7.85
High privacy rating[b] * Job app[c]	2.51	0.66	0.507	−4.89 to 9.91
High privacy rating[b] * Dating app[c]	−0.93	−0.25	0.801	−8.15 to 6.29
Friends' recommendation[a] * High privacy rating[b]	10.41	2.84	0.005**	3.26 to 17.56
Friends' recommendation[a] * High privacy rating[b] * Self-discovery app[c]	−12.35	−2.28	0.023*	−22.94 to −1.76
Friends' recommendation[a] * High privacy rating[b] * Dating app[c]	−6.80	−1.30	0.193	−17.01 to 3.41
Friends' recommendation[a] * High privacy rating[b] * Job app[c]	−5.67	−1.06	0.290	−16.14 to 4.80
Random Effects				
ICC	0.199			
Observations (Level 1)	2000			
N_{id} (Level-2)	500			
Marginal R^2/Conditional R^2	0.29/ 0.57			

Note. Reference category.
[a] Social Media Platform Recommendation.
[b] Low Privacy Rating.
[c] Messenger App.
* $p < .05$.
** $p < .01$.
*** $p < .001$.

developmental tasks.

In addition to the hypotheses, users' download probability was influenced by *app category* with significant differences in download probability for messenger apps compared to other app categories. We found that both self-discovery apps ($b = 9.36$, 95% CI: [2.56, 16.16], $p = .008$) and job apps ($b = 7.56$, 95% CI: [0.60, 14.52], $p = .034$) led to a higher probability of download than messenger apps. In addition, we found a three-way interaction between *recommendation*, *privacy rating* and *self-discovery apps* (compared to messenger apps, $b = -12.35$, 95% CI: [− 22.94, − 1.76], $p = .023$). To gain deeper insight into the three-way interaction, we split the data for *recommendation* and *privacy rating* (Sommet & Morselli, 2021). Regression analyses on the split data sets revealed significantly higher probability of download for self-discovery apps compared to messenger apps in all conditions, except for high privacy combined with friends' recommendation (see Table 4). For other app categories, participants did not indicate significantly different download probability ($p > .156$). Finally, the regression analysis revealed a significant effect of *gender*, with women reporting significantly higher download probability than men ($b = 5.63$, 95% CI: [1.19, 10.07], $p = .01$).

2.3. Discussion

Study 1 examined how friends' recommendation and the developmental opportunities provided by different app categories influence young adults' download probability of low and high privacy rated apps.

2.3.1. The role of privacy rating, recommendation and developmental opportunities at the app download stage

Consistent with our *Hypothesis 1*, the results showed that apps with high privacy ratings were more likely to be downloaded than apps with low privacy ratings. This effect of privacy rating was particularly pronounced when apps were recommended by friends compared to a social media platform. The privacy-enhancing effect is consistent with previous research on privacy indicators discussed above (Bock & Momen, 2020; Hughes-Roberts, 2015) and highlights that participants considered privacy risks in their risk-benefit calculation when downloading apps.

We also proposed that a friend's recommendation would lead to higher download probability compared to a social media platform recommendation for both high- and low-privacy apps (*Hypothesis 2*). Our results confirmed this and are consistent with previous findings on social influence during app downloads mentioned above (e.g., Barth et al., 2019; Harborth & Pape, 2021; Kroschke & Steiner, 2017). This finding suggests that young adults' app download and associated privacy decision is influenced by their peer group and the tendency to imitate the behavior of relevant others (Acquisti et al., 2020). In addition, social benefits such as connecting to ones' peer group through following their recommendation could be valued as an immediate benefit in our study (Acquisti et al., 2020; Lünich et al., 2021).

To further identify benefits particularly relevant to young adults, we examined the influence of app categories that offer different developmental opportunities on young adults' privacy decisions at the app download stage. Given that this user group faces a range of different developmental tasks (Havighurst, 1948; Seiffge-Krenke, 2015), we proposed that apps aligned with unfulfilled and/or important developmental tasks increase download probability compared to apps aligned with fulfilled or unimportant tasks, regardless of the app's privacy rating (*Hypothesis 3*). This assumption was built on the framework of Barth and de Jong (2017). We assumed that apps aligning with relevant developmental tasks might lead young adults to a developmentally driven overestimation of the expected benefit and increase privacy trade-offs among young adults at the app download stage. However, the expected effect was not confirmed. While this finding seems contradictory

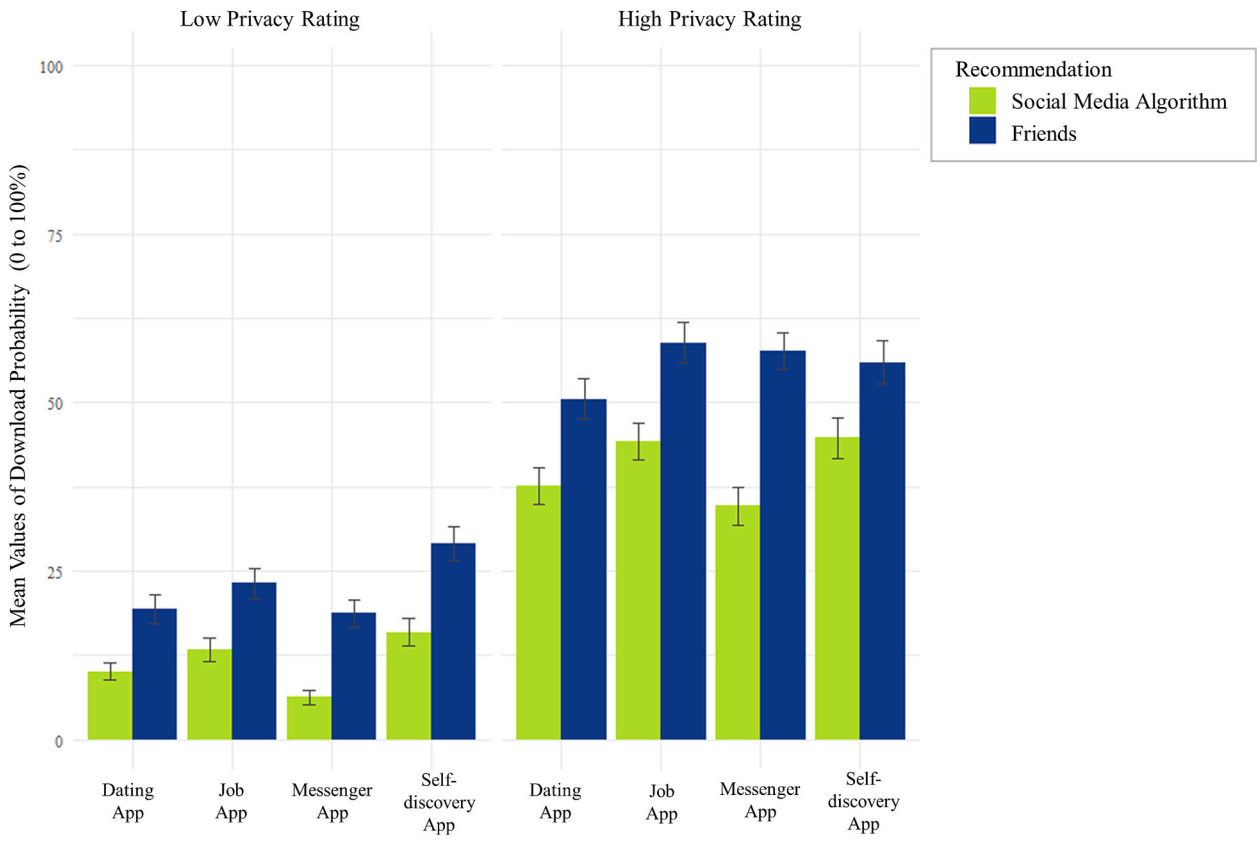


Fig. 5. Mean values of download probability for recommendation (social media platform vs. friends), privacy rating (low vs. high) and app category (job vs. partner vs. self-discovery vs. messenger app). Error bars indicate the standard error of the mean values.

Table 4
Split data analysis of the three-way interactions for download probability (DV) and the predictor self-discovery compared to messenger apps.

Split data on…	Coeff.	*t*-value	p	CI
…low privacy rating & social media platform recommendation	9.74	4.60	<0.001***	5.58 to 13.91
…high privacy rating & social media platform recommendation	9.67	2.39	0.02*	1.71 to 17.64
…low privacy rating & friends' recommendation	9.99	3.14	0.002**	3.74 to 16.24
…high privacy rating & friends' recommendation	−2.26	−0.53	0.595	−10.59 to 6.07

Note.
* $p < .05$.
** $p < .01$.
*** $p < .001$.

to previous research on a developmental perspective (cf. Peter & Valkenburg, 2011; Steijn, 2014; Steijn & Vedder, 2015), it could be explained by our sample, the perceived app importance or its measurement: As our sample showed an overall high importance rating with 93.2% of participants rating the addressed developmental tasks as important, the ability to detect differences in overall consistent responses may be limited. In addition, although we systematically varied developmental opportunities and included relevant information in the scenario and app store depictions, we did not directly assess whether participants personally perceived the app as helpful for accomplishing this task. It is possible that some participants did not consider the app relevant to their own developmental needs. Another reason may be our binary classification of developmental tasks as fulfilled/not fulfilled, which may not capture the full complexity of these tasks because young adults could pursue further career paths or social connections even after starting their first job or belonging to a circle of friends. Future research is needed to compare the process by which information disclosure occurs among different age groups (Anaraky et al., 2021), such as the moderating effects of age on the perception of benefits in developmental and non-developmental contexts. This could provide further experimental insight into the reported null findings in Study 1.

2.3.2. *Exploratory differences in messenger apps and gender*

While we found no differences across the majority of app categories, our results showed that participants indicated a lower probability to download messenger apps compared to self-discovery apps and job apps. With WhatsApp dominating messenger app usage (used by 97.8% of our participants and the most popular app in this category globally; Kemp, 2024), participants may have preferred familiarity and avoided downloading less familiar messenger apps. This is consistent with Bock and Momen (2020), who found that users tend to choose familiar messenger apps such as WhatsApp and ignore privacy indicators for such apps. Even if we counterbalanced our app designs in color to avoid systematic effects of app design as investigated in previous studies (Burgers et al., 2016), our findings across app categories are exploratory and future research could further investigate the effects of app category in different age groups under controlled app designs. Finally, our results showed that women compared to men reported a higher probability to download the apps presented. It could be argued that women engage in higher app downloads and are more likely to accept privacy risks. However, the literature has often examined opposite findings, showing that men engage in riskier online behavior and have fewer privacy concerns than women (Tifferet, 2019). An alternative explanation thus may lie in our study design and the app categories selected. The current literature highlights that women are more likely to engage with most social media

services, for example, by spending more time online or posting more updates (Tifferet, 2019). In addition, women tend to differ in their app usage behavior, for example, by being more likely to download app categories such as e-commerce and relational apps (Kim et al., 2015). While we selected app categories to provide cross-cutting developmental opportunities for young adults, the selected app categories may have held greater relevance for women, explaining their increased app download behavior. It should also be noted that, even though our findings align with previous research, the high prevalence of university students (80%) and women (79.6%) in Study 1 limit the generalization of our findings to a broader population. While we statistically controlled for gender effects, more research is needed to determine if young adults across heterogeneous samples engage in similar privacy trade-offs or face other user-specific privacy challenges.

3. Study 2

While Study 1 extends previous research by examining the trade-offs for both social and developmental benefits between low and high privacy rated apps, Study 2 examines trade-offs for social benefits between low and high privacy rated apps and the role of resignation within a broader age sample. Study 2 focuses on whether social benefits, found highly impactful in Study 1, extend beyond the age group of young adults, while also exploring the role of resignation among young adults and adults. We examine the app category of cooking, which is not directly related to a specific developmental opportunity. This decision was made for a number of reasons: First and foremost, privacy decisions for apps that would be directly related to developmental opportunities may inadvertently reinforce age-related effects, as young adults may perceive them as more beneficial compared to other users. Second, we believe that the binary assessment of developmental fulfillment in Study 1 may not capture the full complexity of developmental processes. Future research using a qualitative approach, such as semi-structured interviews, could provide deeper insights into these dynamics. Due to this non-developmental context, we focused on young adults (18 to 29 years) rather than including those transitioning from adolescence to young adulthood (16- and 17-year-old) in Study 2. In addition, Study 2 employs a 10-item scale measuring participants' probability of disclosing different types of data (e.g., gender, standard web browser) to an app. While the dependent variable of Study 1 was chosen for its parsimony, the single-item measure of probability to download may have oversimplified the complexity of privacy judgments. For example, it did not consider actual data disclosures during app downloads or the perceived sensitivity of different data types. By measuring the probability of disclosing ten different types of data in Study 2, we aim to address this limitation and extend our findings for permission-related concerns rather than the all-or-nothing download decision (Barth et al., 2019). In addition, this shift in methodological design helps us to gain deeper insight into the observed gender differences, which are found heterogenous in privacy research and likely to be influenced by the methodological design (for a meta-analysis, see Tifferet, 2019). Finally, Study 2 extends the research findings of Study 1 by examining how the level of resignation affects young adults' and adults' app privacy decisions and by providing qualitative insights into what is important to users when downloading an app or disclosing data in the given app scenarios. Our goal is to provide a deeper understanding of how resignation affects data sharing at the app download stage among young adults and adults. To achieve this, we provide empirical insights from experimental online vignette studies and examine the prevalence of resignation between different age groups.

Similar to Study 1, we propose the privacy-enhancing effect of privacy ratings, where high ratings lead to an increased probability of data disclosure compared to low ratings (*Hypothesis 1*). We also propose that a friend's recommendation leads to increased probability of data disclosure compared to no recommendation (*Hypothesis 2*). Previous research suggests that young adults might perceive access to certain types of data as less severe (Bemmann & Mayer, 2024) and experience higher levels of privacy cynicism associated with higher resignation (Schomakers et al., 2019; van Ooijen et al., 2024). Additionally, they tend to disclose more personal data to facilitate belonging to their peer group (Steijn, 2014). In light of these findings, we propose that young adults show an increased probability of disclosing data compared to users above 29 years (*Hypothesis 3*). Previous research has emphasized the importance of resignation, highlighting reduced privacy protection behavior among users with higher resignation (Lutz et al., 2020). We propose similar effects, with users reporting higher levels of resignation showing an increased probability of data disclosure compared to users reporting lower levels of resignation (*Hypothesis 4*) and exploratively investigate its prevalence among younger users. Finally, we explored differences in the probability of data disclosure for individual differences in mistrust, uncertainty and powerlessness (other facets of privacy cynicism) and gender differences.

3.1. Method

We conducted an online experimental vignette study with users between 18 and 69 years. The app scenarios included image-based app store depictions of cooking apps and text-based descriptions of them being found when browsing online or recommended by friends (*recommendation*, within-subject). Apps were presented with low or high privacy ratings (*privacy rating*, within-subject). After each scenario, we asked participants to indicate the probability of disclosing different types of data in order to use the app for free from 0% (not at all) to 100% (quite sure) as DV.

3.1.1. Participants

149 participants were recruited via e-mail, social media or direct inquiries. Students from one university received course credit for participation. One participant had to be excluded due to uninterpretable age indication ($N_{\text{excluded}} = 1$). The final sample consisted of 148 participants between 18 and 69 years (105 women, 40 men, 3 no indication; $M = 33.2$ years, $SD = 15.2$). Most participants were university students (51.4%) followed by employees (37.8%). Most participants indicated to download apps less than once a month (62.2%), followed by once (25.7%) and twice a month (10.1%).

3.1.1.1. Ethics and informed consent. Study 2 is a follow-up study of Study 1, which was approved by the ethical committee of HSD Hochschule Döpfer (BEth_20_22, decision of May 19, 2022). No ethical concerns were raised regarding Study 1 or methodically similar follow-up studies with a comparable experimental vignette design. Since this applies to Study 2, no additional ethics board approval was sought. All participants provided informed consent prior to participation. Participants agreed to the privacy protection regulations and their anonymized and aggregated data being stored and published in a data repository. Due to the high standard of privacy protection applied, none of their data was identifiable after collection. Participation was voluntary, and participants retained the right to withdraw at any time.

3.1.1.2. Power analysis. We conducted an a-priori power analysis based on Arend and Schäfer (2019) using the *simr* package in RStudio (RStudio Team, 2022) to estimate the sample size required. For our within-subject design, we assumed medium Level 1, Level 2 direct effects under a high ICC of 0.50. The analysis indicated a minimum of 94 participants to achieve a power greater than 0.80. We maximized the sample size within the study period to increase the informational value of our study.

3.1.2. Procedure

The procedure of Study 2 is visualized in Fig. 6. After the welcoming and informed consent, participants were instructed on the study task and completed a practice trial. Throughout the study, participants received

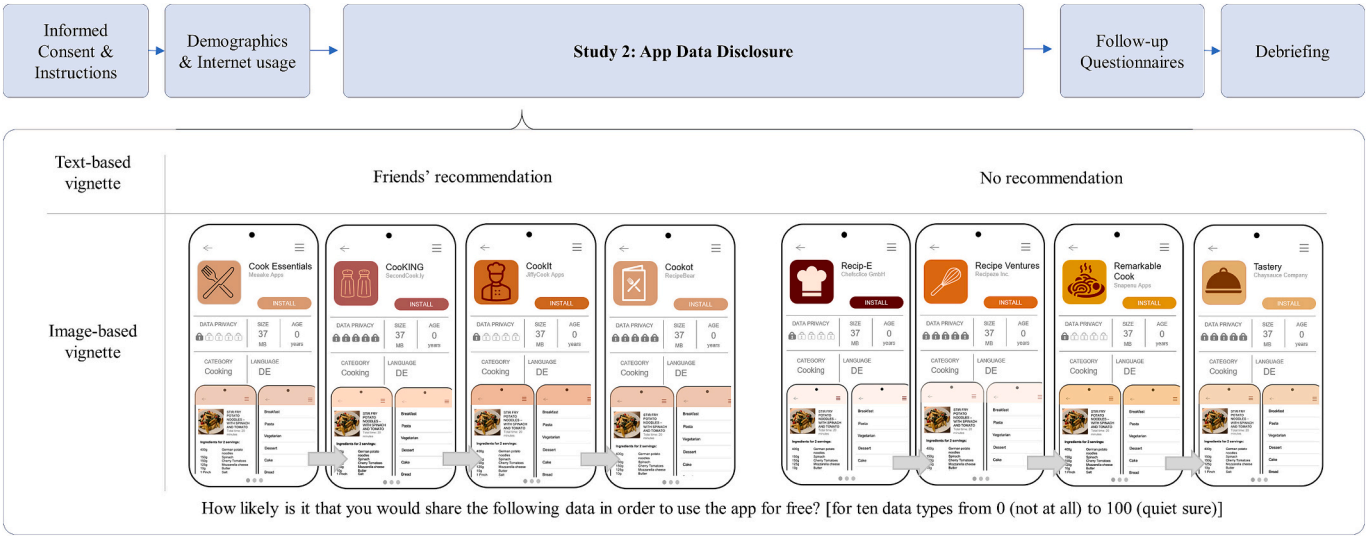


Fig. 6. Overview of the procedure of study 2.
Note. The app designs in Study 2 were counterbalanced for privacy rating and recommendation to avoid systematic effects of app design.

Table 5
Translated text-based scenario for no and friends' recommendation.

Recommendation	Short-text scenario
No	You enjoy trying new recipes when you cook. As you browse through the Internet, you coincidentally see the app [name], which can be used to find delicious recipes. You consider downloading it and take a look at the app with the following information in the app store:
Friend	You enjoy trying new recipes when you cook. While talking about cooking with your friends, they enthusiastically tell you about the new app [name], which helps you find delicious recipes. Your friends offer to share their collective recipe list with you, when you download the app. One friend shows you the app with the following information in the app store:

eight vignette scenarios (see Section 3.1.3). The first four scenarios were presented with either no or a friend's recommendation. After four scenarios, participants were told that the text-based scenario would change and the other recommendation condition was presented. In the vignette scenarios, participants indicated how likely they would be to disclose ten different types of data (e.g. gender, degree) in order to use the app for free on a scale from 0% to 100%. After completion of all vignette scenarios, follow-up questionnaires were queried (see Section 3.1.4) and participants were able to provide study feedback. In the debriefing, participants received detailed information on the study aim. The whole study took approximately 25 min and was conducted using the online tool LimeSurvey (LimeSurvey GmbH, n.d.).

3.1.3. *Vignette scenarios*

Participants received eight image-based app store screens with a similar image-based app store design as Study 1. Similar to Study 1, apps were presented with text-based scenarios, in which apps were found when browsing online (no recommendation) or were recommended by friends (friends' recommendation, see Table 5). Privacy was also indicated with one of five locks for low privacy and five of five locks for high privacy by a simple privacy indicator from Stöver et al. (2021) (see Fig. 7). In contrast to Study 1, each condition was shown two times to increase measurement accuracy resulting in eight app store visualizations per participant, four recommended by friends and four found when browsing online, with two apps of each recommendation condition assigned a low privacy rating and two apps assigned a high privacy rating. To avoid presenting the same app, apps varied in their app design (e.g., icon), which was counterbalanced for privacy rating and



Fig. 7. Translated examples of the image-based app store depictions for a cooking app with low as well as high privacy rating.

recommendation as well as balanced in color to avoid systematic effects of app design. For each app scenario, we asked participants to indicate the probability of disclosing different types of data in order to use the app for free on a scale from 0% to 100% and queried ten data types: (1) residence town/city, (2) entered search terms, (3) gender, (4) standard web browser, (5) country, (6) webpages visited, (7) family status, (8) level of education, (9) height and (10) hobbies. As previous research has highlighted that users' willingness to disclose personal data is influenced by its sensitivity and context (Bansal et al., 2016; Klütsch, Böffel, et al., 2024), the requested data types were chosen to be apparently irrelevant to the apps' functioning and, in line with Leon et al. (2013), of low to medium sensitivity. A follow-up questionnaire (see Section 3.1.4) on data sensitivity confirmed a perceived medium sensitivity of all data

Table 6
Results of the final multilevel linear regression for probability of data disclosure (DV) predicted by recommendation (no vs. friends), privacy rating (low vs. high), young adults (vs. other age groups) and resignation.

Predictors	Coeff.	*t*-value	p	CI
(Intercept)	16.57	6.89	<0.001***	11.88 to 21.27
Friends' recommendation[a]	3.19	3.55	<0.001***	1.43 to 4.95
High privacy rating[b]	9.06	10.08	<0.001***	7.30 to 10.82
Friends' recommendation[a] * High privacy rating[b]	0.43	0.34	0.733	−2.06 to 2.92
Young adults (18 to 29 years)[c]	8.48	2.77	0.006**	2.49 to 14.46
Resignation	7.18	5.62	<0.001***	4.69 to 9.68
Random effects				
ICC	0.733			
Observations (Level 1)	1184			
N_{id} (Level 2)	148			
Marginal R^2/Conditional R^2	0.22/ 0.79			

Note. Reference category.
[a] No recommendation.
[b] Low privacy rating.
[c] Older than 29 years.
* $p < .05$.
** $p < .01$.
*** $p < .001$.

types ($M = 3.30$ to 5.31). All probabilities of disclosed data types were averaged to one mean probability score of data disclosure per scenario.

3.1.4. Follow-up questionnaires

We administered 22-items[2] of the privacy cynicism questionnaire by Lutz et al. (2020) with its subfacets mistrust (6 items), uncertainty (6 items), powerlessness (5 items) and resignation (5 items) on a 7-point Likert scale (1 = strongly disagree, 7 = strongly agree). All subscales reached an acceptable Cronbach's alpha between $\alpha = 0.77$ and $\alpha = 0.88$. Sociodemographic details (e.g., age, gender) and app downloads per month were queried. Additonally, participants were asked in an open-ended question what is important to them when downloading an app in general and on a Likert scale from 1 (not at all) to 7 (strongly) what information (e.g., privacy locks, app category) was important for their data disclosure in the app scenarios. Lastly, the perceived data sensitivity of the data requested in the given app scenarios was assessed on a Likert scale from 1 (not at all) to 10 (strongly) based on Milne et al. (2017).

3.2. Results

The statistical software RStudio (RStudio Team, 2022) was used for analysis. To analyze the dependent variable, *probability of data disclosure*, the probabilities of disclosing the ten different data types were summarized and averaged to obtain one mean probability score of data disclosure per scenario. Given the repeated measures design and an intra-class coefficient (ICC) indicating that 73.3% of the variance in *probability of data disclosure* was explained by between subject differences, a multilevel structure was necessary. We ran multilevel linear regression for *probability of data disclosure* using the lme4 package (Bates et al., 2024). All predictors (except the sub-facets of privacy cynicism) were dummy coded as dichotomized variables. The mean score of each sub-facet of privacy cynicism was added as a single predictor to the regression analysis, with each sub-facet being grand-mean centered. Significance was tested at $\alpha = 0.05$.

The experimental variables *privacy rating* (low vs. high) and *recommendation* (no vs. friends), including their interaction effects, were added to the final multilevel regression analysis. In addition, the hypothesized predictors *resignation* and *young adults*[3] (18 to 29 years vs. older than 29 years) were added as single predictors to the final multilevel regression analysis. Finally, exploratory predictors including the other sub-facets of privacy cynicism (mistrust, powerlessness, uncertainty) and gender were tested to determine if they improved the model fit. All of these exploratory predictors did not significantly improve model fit ($p > .13$) and were therefore not added to the final multilevel regression analysis.

3.2.1. Final multilevel linear regression

The final multilevel linear regression contained the following predictors: *recommendation* (no vs. friend), *privacy rating* (low vs. high), along with their interaction effects as well as *young adults* (young adults vs. other age groups) and *resignation*. Table 6 summarizes the results of the final multilevel linear regression.

In line with *hypothesis 1*, the analysis revealed the proposed effect of *privacy rating* (see Fig. 8): Apps with a high privacy rating led to a higher probability of data disclosure than apps with a low privacy rating ($b = 9.06$, 95% CI: [7.30 to 10.82], $p < .001$). In addition, the proposed effect of *recommendation* was found (*hypothesis 2*): When apps were recommended by friends, the probability of data disclosure to these apps was higher than when apps were not recommended ($b = 3.19$, 95% CI: [1.43 to 4.95], $p < .001$). In contrast to Study 1, no significant interaction effect between *recommendation* and *privacy rating* was found ($b = 0.43$, 95% CI: [−2.06 to 2.92], $p = .73$), suggesting that friends' recommendation did not influence data disclosure as a function of high or low privacy ratings. Confirming the proposed effect of age, we found that *young adults* showed higher probabilities of data disclosure to the presented apps than other age groups above 29 years ($b = 8.48$, 95% CI: [2.49 to 14.46], $p = .006$). We also found the proposed effect of *resignation*: Users who reported higher levels of resignation also showed higher probabilities of data disclosure to the presented apps than users

[2] After data collection, we discovered that the following item had been inadvertently omitted from the subfacet mistrust: "Large Internet companies do with our data what they want". Notably, this item had been excluded by Lutz et al. (2020) for better model fit in the structural equation model due to low loadings or high correlation with similar items. As all subfacets, including mistrust (Cronbachs' $\alpha = 0.85$), also revealed high internal consistency, we retained this subfacet in our exploratory analysis.

[3] We tested for the effect of the continuous variable age to check for robustness of this comparison between younger users aged 18 to 29 years and users above 29 years (see Appendix A.2, Table A.2). The results confirmed that the effect remains consistent when age is treated as a continuous measure ($p = .001$).

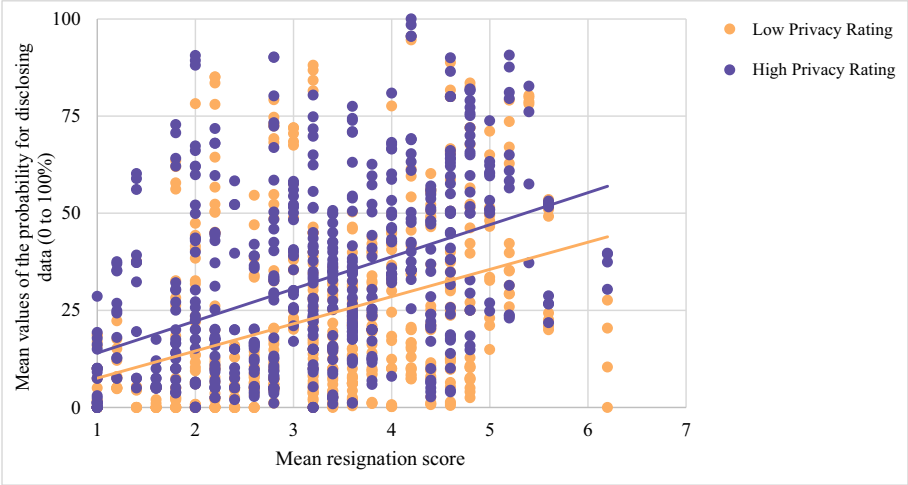


Fig. 8. Mean values of probability for disclosing data for privacy rating (low vs. high) and resignation.

Table 7
Mean values and standard deviation of information considered important for participants' data disclosure in the given app scenarios.

How important was the following information to you in your decision to share your data with the presented apps?	M	SD
Privacy through locks	5.81	1.63
App Size	2.76	1.85
Age rating	2.43	1.77
App category	2.98	1.94
App language	3.73	2.17
App icon	3.09	1.90
App name	2.98	1.83
App manufacturer	3.03	1.93
App preview	3.75	1.90
Friends	4.25	1.73
Advertisement online	2.88	1.62

who reported lower levels of resignation ($b = 7.18$, 95% CI: [4.69 to 9.68], $p < .001$). To assess the relationship between *age* and *resignation*, a Pearson correlation analysis was conducted. The results revealed a significant negative correlation ($r\ (146) = -0.19$, $p = .02$).

3.2.2. Participants download and data disclosure considerations

Table 7 summarizes the descriptive means and standard deviations of the information deemed important for data disclosure in the given app scenarios. Open-ended responses on what is generally considered important when downloading an app were coded by two independent raters into one or more categories. Most participants ($n = 57$) highlighted privacy-related aspects as important criteria for downloading an app. This was followed by social influences such as app recommendations or reviews ($n = 53$) as well as the app's overall benefit ($n = 48$). Additionally, several participants stated that cost ($n = 29$) and the storage capacity ($n = 17$) were important criteria for downloading an app. Furthermore, app-related information, such as the design ($n = 22$), provider information ($n = 20$), professional appearance ($n = 5$), description ($n = 4$) and language ($n = 3$) as well as the ease of use ($n = 20$), in-app advertising ($n = 11$) and transparency ($n = 9$) were stated as important for their app downloads. Some participants stated that security ($n = 14$) and downloading from an official app store ($n = 4$) were important criteria for downloading apps. Lastly, 15 participants provided open answers that were coded as "other", citing isolated aspects such as the speed ($n = 1$), data volume required ($n = 1$) or child protection ($n = 1$) as criteria to download an app.

3.3. Discussion

Similar to Study 1, high privacy ratings in Study 2 also led to an increased probability of data disclosure compared to low privacy ratings (*Hypothesis 1*). Moreover, the recommendation from a friend was found to increase the probability of data disclosure compared to no recommendation (*Hypothesis 2*). In addition, Study 2 extends the findings of Study 1 showing that young adults reported a higher probability of disclosing data compared to users above 29 years (*Hypothesis 3*). This vulnerability could be explained by increased resignation of younger users: Our results showed that users who reported higher levels of resignation also showed a higher probability of disclosing data than users who reported lower levels in resignation (*Hypothesis 4*). With this, our findings confirm insights by Lutz et al. (2020): While mistrust, powerlessness and uncertainty are important facets of privacy cynicism, these facets did not affect intended data sharing with apps in our study. Instead, privacy resignation univocally reduced data protection highlighting resignation as an important factor to address in future interventions. At the same time the level of resignation was negatively correlated with participants' age – a finding that aligns with previous research on privacy cynicism (Schomakers et al., 2019; van Ooijen et al., 2024). It underscores the prevalence of resignation among younger users, suggesting it more pronounced among younger adults and might be increasing their online data disclosure.

Similar to Study 1, it should be noted that Study 2 also included a high proportion of university students (51.4%) and women (70.9%) that reduces its ecological validity. Yet, the comparison of the gender effects in both studies reveals that Study 2 cannot confirm the differences between women and men that were found in Study 1. This finding supports the idea that the app categories in Study 1 may be more relevant to women. However, it can also be explained by methodological differences in both studies. While Study 1 assessed the probability of downloading an app, Study 2 assessed the probability of disclosing certain types of data (e.g., standard web browser). Gender differences might have diminished as the focus shifted towards permission-related concerns. Both explanations would align with previous research highlighting gender differences in privacy decisions as context-dependent and likely to be influenced by methodological design choices (for a meta-analysis, see Tifferet, 2019).

4. General discussion

Two experimental online vignette studies were conducted to investigate which factors lead users, particularly young adults, to privacy trade-offs during the app download stage. Both studies showed that

privacy indicators with simple privacy locks can prompt young adults and adults to consider privacy when downloading apps and protecting their data. Similar to previous studies (Bock & Momen, 2020; Garcia et al., 2025; Meier & Krämer, 2024), our findings underscore that privacy ratings can increase the salience of privacy risks during app download in our sample. At the same time, friends' recommendation was found an important aspect that participants encountered. Considering the pronounced effect of friends' recommendation in high rated privacy apps, young adults and adults may benefit from technical solutions that utilize social comparison mechanisms in a privacy-supportive way. For instance, social reporting systems could enable users to report privacy-invasive practices (Seberger et al., 2021), while social norm nudges could highlight other users' privacy-preserving choice (Masaki et al., 2020). Our findings suggest that, when harnessed constructively, social influence can act as an opportunity; however, it can also act as a risk when reinforcing conformity pressure.

Both studies show that friends' recommendation reduce the beneficial effect of privacy ratings. The open-ended responses of Study 2 illustrate that users valued privacy but also valued social information (e.g., peer recommendations, app ratings) or immediate functional benefits. Previous research has shown that such behavior is accentuated at the app download stage because privacy information is often hidden from the user behind scrolling (Barth et al., 2019; Gu et al., 2017). While providing users with easily accessible privacy information can reduce the uncertainty they encounter (Acquisti, 2004; Acquisti et al., 2017; Barth & de Jong, 2017), awareness of risks alone seems insufficient to enhance privacy protection in social situations. In both studies, participants tended to imitate the behavior of relevant others, valuing recommendations from friends as immediate social benefits that outweighed privacy risks (*present bias*; see also Acquisti et al., 2020; Lünich et al., 2021). While this effect may be exacerbated by simple privacy indicators that expose participants to uncertain and abstract privacy risks, the strong influence of friends' recommendation confirms that the usage behavior of others and social pressure remain challenges to users' privacy across different age groups. Related studies support this finding, highlighting that users often cite the usage behavior of others and social pressure as the main reasons for compromising their privacy across different social technologies (Seberger et al., 2021; Westin & Chiasson, 2021). Future research is needed to investigate whether technical, educational or even regulatory interventions can balance the risk-benefit calculations of users under high social pressure.

This is particularly important as social pressure likely increases feelings of resignation as well: Social networks are often embedded in users' lives, forcing them to engage and depriving them of the power to control their data, which may increase resignation (Lutz et al., 2020; Seberger et al., 2021). Such dynamics may be particularly challenging for younger users who not only experience pronounced FoMO (Przybylski et al., 2013) but also consider belonging to their peer group as a salient developmental task (Havighurst, 1948). Study 2 demonstrated that younger participants reported both higher data disclosure tendencies and stronger feelings of resignation than older participants. Future work should therefore aim to disentangle the individual and contextual factors that contribute to young adults' privacy resignation. As outlined above, social constraints and pronounced FoMO may serve as one explanatory pathway. However, previous research also suggests that educational deficiencies could likewise intensify resignation (Respi et al., 2025). At the same time, researchers point out that simply providing information about online privacy threats may not be enough to overcome resignation and could even increase feelings of resignation (Draper & Turow, 2019; Hoffmann et al., 2016). We encourage future research to include heterogenous samples to expand our findings and gain deeper insight into the individual and contextual factors that contribute to resignation among young adults.

4.1. Practical implications and avenues for future interventions

Our research provides insight into important factors that shape privacy trade-offs among users, particularly young adults, at the app download stage. First, our study confirms previous research that privacy indicators, such as privacy locks, help users integrate privacy-related risks during this stage. We encourage app providers to implement clear, easily understandable privacy indicators like those in our design to help privacy-conscious users to integrate this information at the app download stage. While our findings underscore that social benefits, such as recommendations from friends, can encourage the selection of high privacy-rated apps, they also demonstrate that such recommendations can pose a privacy risk by encouraging the selection of privacy-invasive apps or sharing data with such apps. Our findings underscore the need for future interventions that support users in social situations involving conformity pressure. Furthermore, our findings suggest that younger users and those with higher levels of resignation may be particularly vulnerable to privacy risks, as they were found to express higher probabilities of data disclosure compared to other participants. This underscores the importance of supporting younger and resigned users in future interventions. Building upon previous research, younger and resigned users may benefit from developing technical, educational or even regulatory interventions that (a) promote knowledge and self-efficacy and (b) reduce structural coercion to use certain services.

Lacking knowledge was found to be an important antecedent to resignation in previous research (see, van der Schyff et al., 2023, for a review), with resigned users found to exhibit lower levels of education (Respi et al., 2025). This underscores the need for educational interventions. To avoid contrary effects, future research could investigate the effectiveness of risk information with actionable strategies to foster *self-efficacy,* an attitude known to increase privacy protection despite feelings of resignation (van Ooijen et al., 2024). Personalized Privacy Assistants (PPAs), in the form of a smartphone app, present one promising technical intervention in this regard because it allows users to personalize them according to their individual preferences and needs (Stöver et al., 2023). Marky et al. (2024) examined user preferences for three levels of autonomy: (1) notification PPAs, where users make the decision; (2) recommendation PPAs, where a decision is recommended to users; and (3) decision PPAs, where a decision is made for users. Although the researchers found that users prefer recommendation PPAs (Marky et al., 2024), the theoretical insights on the concept of *privacy cynicism* and *digital resignation* suggests that resigned users could benefit from a mixture of recommendation PPAs that provide step-by-step guidance with decision PPAs that make privacy decisions in regard of the user to reduce cognitive load. In addition, researchers underscore the need to reduce the structural coercion that users experience when using digital services (Draper & Turow, 2019). While app stores integrate reviews of others to the apps usability and services, Seberger et al. (2021) highlight the need to implement social reporting systems that make privacy-invasive practices visible and collectively discussable, especially for apps that are functionally or socially embedded in users' lives. Such systems could help users to resist conformity pressure by making others' privacy concerns visible and by supporting the aggregation of reports on privacy-invasive data practices, thereby enabling collective action (Seberger et al., 2021). They could complement regulatory restrictions and sanctions aimed at limiting privacy-invasive data practices. However, future research is needed to establish how these and other technical, educational, or regulatory interventions could facilitate informed and self-determined privacy decisions online.

4.2. Limitations

Limitations need to be considered when interpreting the results and deriving (methodological) considerations for future research. First and foremost, although the vignettes allowed us to measure app download decisions in a controlled manner, they may not capture the entire

complexity of real-world app download and privacy decisions. This may limit the ecological validity of our findings. We recommend that future studies complement our findings with simulations on real smartphones and consider effects of social influence with confederates in lab experiments. This may be of particular research interest as realistic social influence through confederates could further decrease the consideration of privacy indicators.

Another limitation is shown in the open-ended responses of Study 2. While most participants highlighted privacy-related aspects as important criteria for downloading an app, it cannot be ruled out that the study's framing and context made privacy more salient to our participants than it does in daily interactions with apps in the app store.

Additionally, our research may be limited due to the demographic scope in both studies. Although we statistically controlled for gender differences, the high prevalence of women and highly-educated users in our sample limit its generalizability to a broader population, particularly beyond the WEIRD society (Western, Educated, Industrialized, Rich, and Democratic). While several studies highlight heterogenous findings in the role of gender on users' privacy decisions (Tifferet, 2019), future research is needed to explore the identified gender differences in Study 1 and potential moderators. In addition, and as outlined above, future research on heterogenous samples may help to gain deeper insight into individual and contextual factors as well as user-specific vulnerabilities (e.g., privacy literacy) that contribute to feelings of resignation among younger users and delve into the open question of why young adults engage in privacy trade-offs.

Furthermore, it is important to consider methodological limitations arising from the limited comparison between different (non-) developmental app categories in future research. While Study 2 utilized a non-developmental category (cooking app), future research could systematically contrast developmental and non-developmental contexts to provide further insight into the role of developmental benefits in young adults' privacy trade-offs. This might be particularly relevant, as our sample showed an overall high importance rating of the addressed developmental tasks.

In addition to a non-developmental control condition, multi-method approaches that combine qualitative (e.g., focus groups, semi-structured interviews) and quantitative methods (e.g. lab experiments) could also be helpful to capture the complexities of developmental tasks. This is particularly important because the binary format of developmental task fulfillment used in Study 1 may have oversimplified the complexity of this process. Future research could further benefit from sub group analyses within the age group of young adults (e.g., comparing students with early-career professionals) and in-depth analyses of the process by which information disclosure occurs to better understand user-specific vulnerabilities among this age group (e.g., Anaraky et al., 2021).

Finally, we simplified the privacy indicator with low and high levels of privacy locks as a first step in our research. This simplified privacy indicator might compromise the decision quality (Gerber et al., 2017), compared to privacy indicators combined with additional information. Future research is needed to examine whether our results can be confirmed, when privacy indicators are combined with additional information (e.g., Barth et al., 2021) or specific risk communication (e.g., Gerber et al., 2019).

5. Conclusion

Although apps provide numerous benefits to their users, they can also pose significant privacy risks. In two experimental online vignette studies, we investigated different factors that shape privacy trade-offs, particularly among young adults, when downloading apps. While Study 1 found no differences for apps offering relevant developmental opportunities in our sample, it was shown that participants considered privacy ratings when downloading apps and sharing data. Both studies also emphasized the important role of social influences in users' privacy decisions with friends' recommendations increasing download probabilities and data sharing, also for apps rated low in privacy. Study 2 further showed that young adults and users with higher levels of resignation tend to share more personal data online. To support these user groups, we recommend implementing privacy indicators with step-by-step guidance as well as developing educational and regulatory interventions. These interventions could increase self-efficacy among resigned users and reduce structural coercion of digital services. We encourage future researchers to build on our work, for example, by conducting studies with heterogenous samples to expand our findings and gain deeper insight into individual and contextual factors as well as user-specific vulnerabilities (e.g., privacy literacy) that contribute to resignation among younger participants. In addition, future research could examine the potential of educational, technical and regulatory interventions, outlined in previous studies, to support younger and resigned users online.

CRediT authorship contribution statement

Jennifer Klütsch: Writing – original draft, Visualization, Methodology, Formal analysis, Data curation, Conceptualization. **Annika Kreuder:** Writing – review & editing, Methodology, Formal analysis, Conceptualization. **Luise Haehn:** Writing – review & editing, Formal analysis. **Ida Kuck:** Writing – review & editing, Methodology, Formal analysis, Conceptualization. **Christian Böffel:** Writing – review & editing, Methodology, Formal analysis. **Ulrich Frick:** Supervision, Funding acquisition, Formal analysis, Conceptualization. **Sabine J. Schlittmeier:** Writing – review & editing, Supervision, Funding acquisition, Conceptualization.

Funding

This work was supported by the Federal Ministry of Education and Research (Bundesministerium für Bildung und Forschung, BMBF) within the funded project “Adaptively promoting digital competence and sovereignty of adolescents through micro games” [A-DigiKomp: Digitale Kompetenz und Souveränität Adoleszenter durch Micro Games adaptiv fördern; grant number: 16SV8541]. The funders had no role in the study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

We would like to acknowledge the invaluable contributions of our co-author Prof. Ulrich Frick, who sadly passed away while this manuscript was being prepared. His expertise, dedication, and insights were instrumental to the development of this work. We will miss Prof. Frick not only for his passion for research and expert knowledge but also for the guidance and support he provided to our work. We also thank Nina Wirtz for her support within the literature review and data collection.

Appendix A

A.1.

Table A.1
Results of the final multilevel linear regression with the reference category job app and dating app.

Predictors	Coefficient	*t*-value	p	CI
Self-discovery app[c]	1.80	0.49	0.624	−5.36 to 8.96
Dating app[c]	−3.28	−0.94	0.346	−10.04 to 3.49
Self-discovery app[d]	5.08	1.42	0.156	−1.90 to 12.05
Friends' recommendation[a] * Self-discovery app[c]	3.35	0.85	0.397	−4.38 to 11.08
Friends' recommendation[a] * Dating app[c]	−0.53	−0.14	0.890	−7.99 to 6.94
Friends' recommendation[a] * Self-discovery app[d]	3.88	1.00	0.316	−3.67 to 11.43
High privacy rating[b] * Self-discovery app[c]	−2.15	−0.54	0.586	−9.88 to 5.58
High privacy rating[b] * Dating app[c]	−3.44	−0.90	0.368	−10.91 to 4.02
High privacy rating[b] * Self-discovery app[d]	1.29	0.33	0.739	−6.26 to 8.84
Friends' recommendation[a] * High privacy rating[b] * Self-discovery app[c]	−6.68	−1.19	0.233	−17.61 to 4.25
Friends' recommendation[a] * High privacy rating[b] * Dating app[c]	−1.13	−0.21	0.835	−11.69 to 9.43
Friends' recommendation[a] * High privacy rating[b] * Self-discovery app[d]	−5.55	−1.02	0.310	−16.23 to 5.13

Note. Reference category.
[a] Social media platform recommendation.
[b] Low privacy rating.
[c] Job app.
[d] Dating app.

A.2.

Table A.2
Results of the final multilevel linear regression for probability of data disclosure (DV) predicted by recommendation (no vs. friends), privacy rating (low vs. high), age and resignation.

Predictors	Coeff.	*t*-value	p	CI
(Intercept)	21.55	13.64	<0.001***	18.47 to 24.64
Friends' recommendation[a]	3.19	3.55	<0.001***	1.43 to 4.95
High privacy rating[b]	9.06	10.08	<0.001***	7.30 to 10.82
Friends' recommendation[a] * High privacy rating[b]	0.43	0.34	0.733*	−2.06 to 2.92
Age	−0.33	−3.28	0.001**	−0.52 to −0.13
Resignation	6.84	5.35	<0.001***	4.35 to 9.34

Note. Reference category.
[a] No recommendation.
[b] Low privacy rating.
* $p < .05$.
** $p < .01$.
*** $p < .001$.

Data availability

Data can be retrieved at https://doi.org/10.18154/RWTH-2026-03640

References

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM conference on electronic commerce* (pp. 21–29). https://doi.org/10.1145/988772.988777

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., … Wilson, S. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys, 50*(3), 1–41. https://doi.org/10.1145/3054926

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology, 30*(4), 736–758. https://doi.org/10.1002/jcpy.1191

Anaraky, R. G., Byrne, K. A., Wisniewski, P. J., Page, X., & Knijnenburg, B. (2021). To disclose or not to disclose: Examining the privacy decision-making processes of older vs. younger adults. In *Proceedings of the 2021 CHI conference on human factors in computing systems (CHI '21)* (pp. 1–14). https://doi.org/10.1145/3411764.3445204

Appfigures. (2022). *Age group distribution of mobile app users worldwide in the Google play store in 2nd quarter 2022, by category*. Statista. August 29 https://www.statista.com/statistics/1333429/google-play-store-apps-age-distribution-by-category/.

Arend, M. G., & Schäfer, T. (2019). Statistical power in two-level models: A tutorial based on Monte Carlo simulation. *Psychological Methods, 24*(1), 1–19. https://doi.org/10.1037/met0000195

Atzmüller, C., & Steiner, P. M. (2010). Experimental vignette studies in survey research. *Methodology, 6*(3), 128–138. https://doi.org/10.1027/1614-2241/a000014

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management, 53*(1), 1–21. https://doi.org/10.1016/j.im.2015.08.001

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics, 34*(7), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Barth, S., de Jong, M. D. T., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics, 41*, 55–69. https://doi.org/10.1016/j.tele.2019.03.003

Barth, S., Ionita, D., de Jong, M. D. T., Hartel, P. H., & Junger, M. (2021). Privacy rating: A user-centered approach for visualizing data handling practices of online services. *IEEE Transactions on Professional Communication, 64*(4), 354–373. https://doi.org/10.1109/TPC.2021.3110617

Bates, D., Maechler, M., Bolker, B., Walker, S., Christensen, R. H. B., Singmann, H., Dai, B., Scheipl, F., Grothendieck, G., Green, P., Fox, J., Bauer, A., Tanaka, E., &

Jagan, M. (2024). lme4: Linear mixed-effects models using "Eigen" and S4 (version 1.1-35.1) [Computer software] https://cran.r-project.org/web/packages/lme4/index.html.

Bemmann, F., & Mayer, S. (2024). The impact of data privacy on users' smartphone app adoption decisions. *Proceedings of the ACM on Human-Computer Interaction, 8*, 1–23. https://doi.org/10.1145/3676525

Bock, S., & Momen, N. (2020). Nudging the user with privacy indicator: A study on the app selection behavior of the user. In *NordiCHI '20: Proceedings of the 11th Nordic conference on human-computer interaction: Shaping experiences, shaping society* (pp. 1–12). https://doi.org/10.1145/3419249.3420111

Borca, G., Bina, M., Keller, P. S., Gilbert, L. R., & Begotti, T. (2015). Internet use and developmental tasks: Adolescents' point of view. *Computers in Human Behavior, 52*, 49–58. https://doi.org/10.1016/j.chb.2015.05.029

Bösch, C., Erb, B., Kargl, F., Kopp, H., & Pfattheicher, S. (2016). Tales from the dark side: Privacy dark strategies and privacy dark patterns. *Proceedings on Privacy Enhancing Technologies, 2016*(4), 237–254. https://doi.org/10.1515/popets-2016-0038

Buck, C., Horbel, C., Kessler, T., & Christian, C. (2014). Mobile consumer apps: Big data brother is watching you. *Marketing Review St. Gallen, 31*, 26–35. https://doi.org/10.1365/s11621-014-0318-2

Burgers, C., Eden, A., de Jong, R., & Buningh, S. (2016). Rousing reviews and instigative images: The impact of online reviews and visual design characteristics on app downloads. *Mobile Media & Communication, 4*(3), 327–346. https://doi.org/10.1177/2050157916639348

Caraban, A., Karapanos, E., Gonçalves, D., & Campos, P. (2019). 23 ways to nudge: A review of technology-mediated nudging in human-computer interaction. In *Proceedings of the 2019 CHI conference on human factors in computing systems* (pp. 1–15). https://doi.org/10.1145/3290605.3300733

Coyne, S. M., Padilla-Walker, L. M., & Howard, E. (2013). Emerging in a digital world: A decade review of media use, effects, and gratifications in emerging adulthood. *Emerging Adulthood, 1*(2), 125–137. https://doi.org/10.1177/2167696813479782

Dogruel, L., Joeckel, S., & Bowman, N. D. (2015). Choosing the right app: An exploratory perspective on heuristic decision processes for smartphone app selection. *Mobile Media & Communication, 3*(1), 125–144. https://doi.org/10.1177/2050157914557509

Draper, N. A., Hoffmann, C. P., Lutz, C., Ranzini, G., & Turow, J. (2024). Privacy resignation, apathy, and cynicism: Introduction to a special theme. *Big Data & Society, 11*(3). https://doi.org/10.1177/20539517241270663

Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. *New Media & Society, 21*(8), 1824–1839. https://doi.org/10.1177/1461444819833331

Garcia, K., Tamo-Larrieux, A., Meier, Y., Mayer, S., Lutz, C., Guitton, C., … Mulders, S. (2025). *Visual privacy: The impact of privacy labels on privacy behaviors online* (Preprint). Open Science Framework. https://doi.org/10.31235/osf.io/5kthu_v1

General Data Protection Regulation. (2016). *Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing*.

Gerber, N., Reinheimer, B., & Volkamer, M. (2019). Investigating people's privacy risk perception. In *, 3. Proceedings on privacy enhancing technologies* (pp. 267–288). https://doi.org/10.2478/popets-2019-0047

Gerber, P., Volkamer, M., & Renaud, K. (2017). The simpler, the better? Presenting the COPING android permission granting interface for better privacy-related decisions. *Journal of Information Security and Applications, 34*, 8–26. https://doi.org/10.1016/j.jisa.2016.10.003

Gu, J., Xu, Y.(C.), Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems, 94*, 19–28. https://doi.org/10.1016/j.dss.2016.10.002

Hansen, P. G., & Jespersen, A. M. (2013). Nudge and the manipulation of choice: A framework for the responsible use of the nudge approach to behaviour change in public policy. *European Journal of Risk Regulation, 4*(1), 3–28. https://doi.org/10.1017/S1867299X00002762

Harborth, D., & Pape, S. (2021). Investigating privacy concerns related to mobile augmented reality apps – A vignette based online experiment. *Computers in Human Behavior, 122*, Article 106833. https://doi.org/10.1016/j.chb.2021.106833

Harkous, H., Fawaz, K., Lebret, R., Schaub, F., Shin, K. G., & Aberer, K. (2018). Polisis: Automated analysis and presentation of privacy policies using deep learning. In *Proceedings of the 27th USENIX security symposium* (pp. 531–548). USENIX Association.

Havighurst, R. J. (1948). *Developmental tasks and education*. The University of Chicago Press.

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10*(4), Article 4. https://doi.org/10.5817/CP2016-4-7

Hughes-Roberts, T. (2015). Privacy as a secondary goal problem: An experiment examining control. *Information and Computer Security, 23*(4), 382–393. https://doi.org/10.1108/ICS-10-2014-0068

Kemp, S. (2024). Digital 2024 April global statshot report. *Data Reportal and We Are Social and Meltwater*. https://datareportal.com/reports/digital-2024-april-global-statshot.

Kezer, M., Sevi, B., Cemalcilar, Z., & Baruh, L. (2016). Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10*(1), Article 1. https://doi.org/10.5817/CP2016-1-2

Kim, Y., Briley, D. A., & Ocepek, M. G. (2015). Differential innovation of smartphone and application use by sociodemographics and personality. *Computers in Human Behavior, 44*, 141–147. https://doi.org/10.1016/j.chb.2014.11.059

Klütsch, J., Böffel, C., Abraham, L., Mooser, J., Thüs, D., Tawanger, P., … Schlittmeier, S. J. (2024). How users make online privacy decisions in work and personal contexts of use. *Scientific Reports, 14*(1), 19849. https://doi.org/10.1038/s41598-024-70718-7

Klütsch, J., Haehn, L., Kreuder, A., Böffel, C., Frick, U., & Schlittmeier, S. J. (2025). InstaTrust or InstaTrap: How relationships and developmental tasks affect young adults' phishing susceptibility on Instagram. *International Journal of Human-Computer Studies, 197*, Article 103456. https://doi.org/10.1016/j.ijhcs.2025.103456

Klütsch, J., Schwab, J., Böffel, C., Zimmermann, V., & Schlittmeier, S. J. (2024). Friend or phisher: How known senders and fear of missing out affect young adults' phishing susceptibility on social media. *Humanities and Social Sciences Communications, 11*(1), 1–14. https://doi.org/10.1057/s41599-024-03412-8

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Kollnig, K., Shuba, A., van Kleek, M., Binns, R., & Shadbolt, N. (2022). Goodbye tracking? Impact of iOS app tracking transparency and privacy labels. In *Proceedings of the 2022 ACM conference on fairness, accountability, and transparency* (pp. 508–520). https://doi.org/10.1145/3531146.3533116

Kreuder, A., Frick, U., Rakoczy, K., & Schlittmeier, S. J. (2024). Digital competence in adolescents and young adults: A critical analysis of concomitant variables, methodologies and intervention strategies. *Humanities and Social Sciences Communications, 11*(1), 1–20. https://doi.org/10.1057/s41599-023-02501-4

Kreuder, A., Haehn, L., Klütsch, J., Schlittmeier, S. J., & Frick, U. (2023). "Cookies? I don't even know what that is." - online focus groups on adolescents' experience and behavior in the digital space. In *, 2023. Proceedings of Mensch und Computer* (pp. 498–502). https://doi.org/10.1145/3603555.3608570

Kroschke, M., & Steiner, M. (2017). The influence of social cues on users' information disclosure intentions – The case of mobile apps. In *ICIS proceedings of the 38th international conference on information systems* (p. 38).

Leon, P. G., Ur, B., Wang, Y., Sleeper, M., Balebako, R., Shay, R., … Cranor, L. F. (2013). What matters to users? Factors that affect users' willingness to share information with online advertisers. *Proceedings of the Ninth Symposium on Usable Privacy and Security, 1–12*. https://doi.org/10.1145/2501604.2501611

LimeSurvey GmbH. (n.d.). LimeSurvey: An open-source survey tool [Computer software]. http://www.limesurvey.org.

Lünich, M., Marcinkowski, F., & Kieslich, K. (2021). It's now or never! Future discounting in the application of the online privacy calculus. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 15*(3), Article 3. https://doi.org/10.5817/CP2021-3-11

Lutz, C., Hoffmann, C. P., & Ranzini, G. (2020). Data capitalism and the user: An exploration of privacy cynicism in Germany. *New Media & Society, 22*(7), 1168–1187. https://doi.org/10.1177/1461444820912544

Marky, K., Stöver, A., Prange, S., Bleck, K., Gerber, P., Zimmermann, V., … Mühlhäuser, M. (2024). Decide yourself or delegate - user preferences regarding the autonomy of personal privacy assistants in private IoT-equipped environments. In *Proceedings of the 2024 CHI conference on human factors in computing systems* (pp. 1–20). https://doi.org/10.1145/3613904.3642591

Masaki, H., Shibata, K., Hoshino, S., Ishihama, T., Saito, N., & Yatani, K. (2020). Exploring nudge designs to help adolescent SNS users avoid privacy and safety threats. In *Proceedings of the 2020 CHI conference on human factors in computing systems* (pp. 1–11). Association for Computing Machinery. https://doi.org/10.1145/3313831.3376666.

Masur, P. K. (2018). *Situational privacy and self-disclosure: Communication processes in online environments*. Springer International Publishing. https://doi.org/10.1007/978-3-319-78884-5

Masur, P. K., Bazarova, N. N., & DiFranzo, D. (2023). The impact of what others do, approve of, and expect you to do: An in-depth analysis of social norms and self-disclosure on social media. *Social Media + Society, 9*(1). https://doi.org/10.1177/20563051231156401

Masur, P. K., DiFranzo, D., & Bazarova, N. N. (2021). Behavioral contagion on social media: Effects of social norms, design interventions, and critical media literacy on self-disclosure. *PLoS One, 16*(7), Article e0254670. https://doi.org/10.1371/journal.pone.0254670

Mehdy, A. K. M. N., Ekstrand, M. D., Knijnenburg, B. P., & Mehrpouyan, H. (2021). Privacy as a planned behavior: Effects of situational factors on privacy perceptions and plans. In *Proceedings of the 29th ACM conference on user modeling, adaptation and personalization* (pp. 169–178). https://doi.org/10.1145/3450613.3456829

Meier, Y., & Krämer, N. C. (2024). The privacy calculus revisited: An empirical investigation of online privacy decisions on between- and within-person levels. *Communication Research, 51*(2), 178–202. https://doi.org/10.1177/00936502221102101

Milne, G. R., Pettinico, G., Hajjat, F. M., & Markos, E. (2017). Information sensitivity typology: Mapping the degree and type of risk consumers perceive in personal data sharing. *Journal of Consumer Affairs, 51*(1), 133–161. https://doi.org/10.1111/joca.12111

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Peirce, J., Gray, J. R., Simpson, S., MacAskill, M., Höchenberger, R., Sogo, H., … Lindeløv, J. K. (2019). PsychoPy2: Experiments in behavior made easy. *Behavior Research Methods, 51*, 195–203. https://doi.org/10.3758/s13428-018-01193-y

Peter, J., & Valkenburg, P. M. (2011). Adolescents' online privacy: Toward a developmental perspective. In S. Trepte, & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 221–234). Springer. https://doi.org/10.1007/978-3-642-21521-6_16.

Popovac, M., & Hadlington, L. (2020). Exploring the role of egocentrism and fear of missing out on online risk behaviours among adolescents in South Africa.

International Journal of Adolescence and Youth, 25(1), 276–291. https://doi.org/10.1080/02673843.2019.1617171

Przybylski, A. K., Murayama, K., DeHaan, C. R., & Gladwell, V. (2013). Motivational, emotional, and behavioral correlates of fear of missing out. *Computers in Human Behavior, 29*(4), 1841–1848. https://doi.org/10.1016/j.chb.2013.02.014

Respi, C., Gui, M., Scaduto, G., Serini, M., Pizzul, D., Gerosa, T., & Lutz, C. (2025). Lower cynicism, not higher literacy, promotes protective behavior: Exploring the "privacy exception" in the digital inequality framework. *Social Science Computer Review.* , Article 08944393251341201. https://doi.org/10.1177/08944393251341201

RStudio Team. (2022). RStudio: Integrated development for R (version 2022.12.10) [R]. RStudio, PBC. http://www.rstudio.com/.

Sawyer, S. M., Azzopardi, P. S., Wickremarathne, D., & Patton, G. C. (2018). The age of adolescence. *The Lancet Child & Adolescent Health, 2*(3), 223–228. https://doi.org/10.1016/S2352-4642(18)30022-1

Schomakers, E.-M., Lidynia, C., & Ziefle, M. (2019). A typology of online privacy personalities: Exploring and segmenting users' diverse privacy attitudes and behaviors. *Journal of Grid Computing, 17*(4), 727–747. https://doi.org/10.1007/s10723-019-09500-3

Seberger, J. S., Llavore, M., Wyant, N. N., Shklovski, I., & Patil, S. (2021). Empowering resignation: There's an app for that. In *Proceedings of the 2021 CHI conference on human factors in computing systems* (pp. 1–18). https://doi.org/10.1145/3411764.3445293

Seiffge-Krenke, I. (2001). *Developmental task questionnaire for young adults (DTQ-YA)*.

Seiffge-Krenke, I. (2015). Experiencing the transition to adulthood in Germany: Including emerging adults of the "forgotten half.". In R. Žukauskienė (Ed.), *Emerging adulthood in a European context* (1st ed., pp. 79–93). Routledge.

Seiffge-Krenke, I., Kreuder, A., & Klütsch, J. (2025). *Entwicklungsaufgaben junger Erwachsener heute: Eine aktualisierte Version des Developmental Task Questionnaire for Young Adults (DTQ-YA-2)*. RWTH Aachen University. https://doi.org/10.18154/RWTH-2025-01284

Simon, H. A. (1955). A behavioral model of rational choice. *The Quarterly Journal of Economics, 69*(1), 99–118. https://doi.org/10.2307/1884852

Sommet, N., & Morselli, D. (2021). Keep calm and learn multilevel linear modeling: A three-step procedure using SPSS, Stata, R, and Mplus. *International Review of Social Psychology, 34*(1), Article 24. https://doi.org/10.5334/irsp.555

Steijn, W. M. P. (2014). A developmental perspective regarding the behaviour of adolescents, young adults, and adults on social network sites. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 8*(2), Article 2. https://doi.org/10.5817/CP2014-2-5

Steijn, W. M. P., & Vedder, A. (2015). Privacy under construction: A developmental perspective on privacy perception. *Science, Technology, & Human Values, 40*(4), 615–637. https://doi.org/10.1177/0162243915571167

Stöver, A., Gerber, N., Kaushik, S., Mühlhäuser, M., & Marky, K. (2021). Investigating simple privacy indicators for supporting users when installing new mobile apps. In *Extended abstracts of the 2021 CHI conference on human factors in computing systems* (pp. 1–7). https://doi.org/10.1145/3411763.3451791

Stöver, A., Hahn, S., Kretschmer, F., & Gerber, N. (2023). Investigating how users imagine their personal privacy assistant. *Proceedings on Privacy Enhancing Technologies, 2023*(2), 384–402. https://doi.org/10.56553/popets-2023-0059

TechCrunch. (2024). *Number of mobile app downloads worldwide from 2016 to 2023 (in billions)*. Statista. January 10 https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/.

Thaler, R. H., & Sunstein, C. R. (2009). *Nudge: Improving decisions about health, wealth, and happiness*. Penguin Books.

Tifferet, S. (2019). Gender differences in privacy tendencies on social network sites: A meta-analysis. *Computers in Human Behavior, 93*, 1–12. https://doi.org/10.1016/j.chb.2018.11.046

Trepte, S., & Masur, P. K. (2023). Definitions of privacy. In S. Trepte, & P. K. Masur (Eds.), *The Routledge handbook of privacy and social media* (pp. 3–15). Routledge. https://doi.org/10.4324/9781003244677-2.

van den Broeck, E., Poels, K., & Walrave, M. (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). https://doi.org/10.1177/2056305115616149

van der Schyff, K., & Flowerday, S. (2023). The mediating role of perceived risks and benefits when self-disclosing: A study of social media trust and FoMO. *Computers & Security, 126*, 103071.

van der Schyff, K., Foster, G., Renaud, K., & Flowerday, S. (2023). Online privacy fatigue: A scoping review and research agenda. *CFuture Internet, 15*(5), 164. https://doi.org/10.3390/fi15050164

van Ooijen, I., Segijn, C. M., & Opree, S. J. (2024). Privacy cynicism and its role in privacy decision-making. *Communication Research, 51*(2), 146–177. https://doi.org/10.1177/00936502211060984

Westin, A. F. (1967). *Privacy and freedom*. Atheneum.

Westin, F., & Chiasson, S. (2021). "It's so difficult to sever that connection": The role of FoMO in users' reluctant privacy behaviours. In *Proceedings of the 2021 CHI conference on human factors in computing systems* (pp. 1–15). https://doi.org/10.1145/3411764.3445104

Windl, M., Henze, N., Schmidt, A., & Feger, S. S. (2022). Automating contextual privacy policies: Design and evaluation of a production tool for digital consumer privacy awareness. In *Proceedings of the 2022 CHI conference on human factors in computing systems* (pp. 1–18). https://doi.org/10.1145/3491102.3517688

Wirth, J., Maier, C., & Laumer, S. (2018). The influence of resignation on the privacy calculus in the context of social networking sites: An empirical analysis. In *Proceedings of the twenty-sixth European conference on information systems (ECIS 2018)* (p. 16).

Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems, 106*, 44–52. https://doi.org/10.1016/j.dss.2017.12.003

Zaeem, R., German, R., & Barber, K. S. (2018). PrivacyCheck: Automatic summarization of privacy policies using data mining. *ACM Transactions on Internet Technology, 53*, 1–18. https://doi.org/10.1145/3127519