12-2022

Empowering Older Adults With Their Information Privacy Management

Reza Ghaiumy Anaraky
rghaium@g.clemson.edu

Empowering Older Adults With Their Information Privacy Management

A Dissertation
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy
Computer Science

by
Reza Ghaiumy Anaraky
Dec 2022

Accepted by:
Dr. Bart P. Knijnenburg, Committee Chair
Dr. Marten Risius
Dr. Kaileigh A. Byrne
Dr. Kelly Caine
Dr. Guo Freeman

Abstract

Literature depicts a deficit-based narrative around older adults and their technology use, suggesting that older adults are not able to keep up with their younger counterparts in adopting new technologies. In this dissertation, I argue that this view is not necessarily accurate or productive. Instead, I argue that the deficit is in the technology design, which is not inclusive and often caters to the needs of younger adults.

I study older and younger adults' privacy decision-making as a showcase. In chapter 3, I show that privacy decisions are malleable to external influences and are not fully rational. Therefore, I used a dual-route approach that, in addition to the traditional privacy calculus, also accounts for decision heuristics. This dual-route approach studies the privacy decision-making process with more granularity and can disentangle different aspects of the decision. This gives us an advantage in identifying older and younger adults' differences in privacy decision-making.

My results rebut the deficit-based narrative and show that older adults are motivated and able to manage their privacy. However, they have a different decision-making mechanism compared to younger adults. For example, in chapter 4 I show that older adults are more likely to make a rational decision by considering a more thorough risk/benefit trade-off than younger adults. In addition, in chapter 5 I show that some dark-pattern design mechanisms put older adults at a disadvantage. For example, setting the defaults on disclosure would elevate older adults' concerns for privacy. Lastly, in chapter 6 I show that some of the effects of age (i.e., being older or younger adult) can be justified by considering the hidden variables on which older and younger adults have significant differences. For example, older adults have significantly different levels of privacy literacy and concerns. These two variables mediate the moderating effect of age on privacy decision-making. My work introduces a new perspective in technology design and has practical implications for designing for the elderly.

Dedication

To my parents, Ali and Ashraf, for their unconditional love, support, and all the sacrifices they made for me,

To my sisters Nasibeh and Samaneh for being a constant source of inspiration and encouragement,

To my American parents, Vernon and Maria, who offered me warmth and love at their home, Rivendell, while I had no family in the US,

And to my friend Bart and all of my other friends in HATLab, who were always reliable support for me

Your support can never be quantified, even with R and Mplus.

Acknowledgments

I would like to express my gratitude to my committee chair and adviser, Professor Bart Knijnenburg, for his mentorship and continuous encouragement to gain new skills and try new methods. I understand that these all came at the cost of his time, sometimes with late-night meetings and prolonged conversations on my projects.

I also thank Professor Fred Switzer, who helped me find my interest in how people make decisions, and Professor Kaileigh Byrne, my Psychology mentor, who welcomed me in her lab and helped me explore this interest further.

Special thanks to my IS mentor, Professor Marten Risius, who helped me see the value of theory and concise writing.

I want to acknowledge my collaborators, Professor Pamela Wisnewski and Professor Xinru Page, who helped shape my research agenda.

I should also express my gratitude to Professor Kelly Caine, who taught me to be critical of my own work.

I'll forever be in debt to Professor Alexander Herzog and Professor Brian Malloy, my teaching role models.

I'm also very grateful to my extraordinary Mentor, Professor Cameron Bushnell, the director of Pearce Center for Professional Communication, for her invaluable support.

I'm very grateful to Professor Shelia Cotten for trusting me to solve different analytical problems.

Last but not least, I thank my other committee member Professor Guo Freeman for helping me with my projects, my eye-tracking expert collaborator Dr. Matias Volonte, and my writing buddy Dr. Byron Lowerns.

I am grateful for the generous financial support from Meta that awarded me a Facebook

Fellowship. This fellowship award helped me focus on my research, attend conferences, and network with scholars. However, this dissertation does not necessarily reflect the view of the funders.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

Technology has dramatically improved both life expectancy and the quality of life. For example, wearable devices are equipped with emergency procedures that can be activated in case of life-threatening situations [275] (e.g., someone falling [283]). Furthermore, they collect health information that can help early disease diagnoses and treatment [200]. In addition, smartphones have the capabilities to monitor health parameters and improve quality of life [180]. Besides physical well-being, technology can also help improve its users' mental well-being. For example, using image-based social media can mitigate loneliness [248]. In general, technologies such as social media foster entertainment, social interactions, and companionship [279]. It is, therefore, not surprising that countries that have a higher investment in the IT sector also have a higher average of life-expectancy [223].

Despite the potential in technology to help everyone, individuals do not benefit from it equally. Older adults are more prone to adverse health conditions than others [104], and experience a high risk of social isolation [230]. While technology can significantly improve the health of older adults [62, 59, 58], their technology usage is much below other populations [86], leading them to miss the vast benefits of technology.

Traditionally, scholars argued that the reason for older adults' low technology usage is their lack of digital literacy [259, 290, 272, 86]. However, more recently my own work and other scholars argued against this: while older adults have a different thinking mechanism compared to other populations [60], the technology is not tailored to them [20, 109]. Indeed, research shows that privacy decision making is one of the cases where older and younger adults follow a different thinking process [20]. In addition, privacy is one of the main concerns for older adults when using the technology [215, 68, 81]. Therefore, there is a need to study older adults' privacy decisions and generate design guidelines to develop better technologies that suit this population.

Studying privacy decisions, however, is difficult as such decisions are complex, and many factors play a role in them. For example, while it is reasonable to think that one considers the risks and benefits of disclosure prior to making the decision [83], this is not the full story [3]. Individuals may subconsciously be influenced by heuristics and environmental cues [7, 146, 150, 19, 167]. Scholars developed several frameworks to confront this complexity and studied privacy decisions in different contexts. While all of these frameworks are valid, no single framework can solely depict a comprehensive view of the dynamics behind privacy decisions. Therefore, I adopt multiple frameworks to study the privacy decision-making of older adults.

1.1 A Dual-route Framework for Studying Privacy

Privacy calculus is one of the first and most popular frameworks for studying privacy decision-making. The idea behind the privacy calculus is simple; individuals first think about the benefits and risks of disclosure and disclose their data only if the benefits exceed the costs. Culnan [83] was the first who used the term "privacy calculus" for this risk-benefit trade-off. Many studies have adopted this framework to study privacy decisions. For example, a survey of 326 high school students showed that perceiving more risk for information disclosure can reduce subjects' willingness to provide information. On the other hand, as respondents perceived disclosure more beneficial, they were more willing to disclose information [334]. In the context of location-based services, for example, perceived benefits of disclosing location (e.g., improving life and work efficiency) are positively associated with behavioral intentions of location sharing. In contrast, the subjective risk perceptions of unpredicted problems that may arise from location sharing are negatively related to location sharing behavioral intentions [288].

However, a big portion of privacy decisions is left unexplained with the privacy calculus framework. Arguably, privacy decisions are not merely a product of a rational process. Despite high prevailing privacy concerns, users sometimes overshare information on social media [12], which might cause unintended consequences [260]. It follows that users' privacy decisions are susceptible to heuristic influences [3, 22]. Therefore, there is a need for integrating heuristic frameworks in privacy studies to cover the shortcomings of the privacy calculus. In this work, I adopt a dual-route framework by considering both the privacy calculus and heuristic aspects to study older adults' decision-making.

1.2 Older Adults' Privacy

A large body of literature investigating age-related differences in digital privacy identifies older adults as individuals who experience more difficulties than younger adults in managing their digital privacy. This difference may justify why, overall, older adults fell behind their younger counterparts in tech usage (e.g., [46, 50, 171, 241, 307]). Older adults are less likely to protect themselves against privacy-related risks [294, 336]. Lack of awareness of the privacy risks has been cited as a critical factor impacting older adults' privacy decisions [199]. For example, age-related differences have been found in research investigating content sharing, and sociability and how these components are associated with the need for privacy among Facebook users [50]. Researchers discovered that younger adults are more competent in their Facebook usage and are more informed about and able to make changes to their privacy settings. In contrast, older adults seemed to have difficulties understanding the privacy settings and be less aware of social privacy issues.

Some scholars, however, do not subscribe to this narrative. They believe that older adults and younger adults follow a different decision-making mechanism. Psychological literature corroborates how older and younger adults exhibit fundamental behavioral distinctions in their decision-making patterns, encompassing differences in risk preference and reliance on goal-driven approaches [327]. These scholars believe that older adults' performance with technology is hindered by the fact that many technologies do not tailor their services to older adult populations [105, 258, 110, 113]. According to this narrative, older adults lack of awareness may heighten their privacy concerns [135], and their low technology use rate can be due to an informed privacy decision (i.e., non-use due to costs outweighing benefits) rather than an inability to learn [171].

Despite this new trend of moving beyond a deficit-based narrative, the literature still does not provide an actionable approach to improve the situation for older adults. Older adults are still being ignored in the technology development process, resulting in technologies that are not friendly to older adults. This is particularly prevalent in the area of privacy. For instance, Brandtzæg et al. [50] interviewed Facebook users about privacy features and found that younger adults can find and understand these features easier compared to older adults. Van den Broeck et al.[307] divided participants aged 18 to 65 into three age groups and found that while the oldest group reported more privacy concerns, younger users used more privacy control features. To address these heightened privacy concerns, older adults sometimes avoid the use of digital technologies, such as social media [250]. Therefore, technology should revise how it presents privacy management mechanisms to older adults and make it more compatible with older adults' decision-making process.

In this work, I take on a strength-based approach and study older adults' privacy behavior with a lens of differences rather than deficits. Indeed, I consider the deficits to be on the technology side and not older adult users, as tech products are not suiting their older adult audiences. This perspective has two significant merits: firstly, it contributes to the theory by viewing the problem of older adults' low tech usage from a different perspective. Secondly, it helps me generate actionable design implications to address the shortcomings in privacy management mechanisms and is a step towards developing older-adults friendly products.

1.3 Age May Be a Proxy

Most of the privacy literature uses the age group as a clustering variable to study older and young adults' decisions and commonly neglects that the actual reason for the differences between young and older adults may not be only due to age; instead, age may act as a proxy for some hidden variables. To have a deeper understanding of older and younger adults' differences, however, we need to move beyond clustering them only by age and be seek out the sources of differences between the two populations. This chapter acknowledges that **the differences between young and older adults are not caused because of age itself, but there are other variables preceding age**. For example, privacy concerns is one of the most important predictors of privacy decisions [277]. Part of the different privacy behavior among younger and older adults may be due to having different levels of privacy concerns [307, 133]. Privacy self-efficacy is another predictor of privacy decisions, where evidence suggests that older adults have lower levels of self-efficacy [133]. Digital privacy literacy is the third variable of my interest. Highly literate individuals are more likely to control their privacy decisions [325]. A significant body of privacy literature considers older adults as individuals with lower levels of digital literacy [47, 310, 301, 16, 107, 272]. However, this assumption is not empirically supported [163]. Therefore, I study digital privacy literacy due to lack of consensus and the importance of the privacy literacy variable. I will discuss these variables further in chapter 2.

1.4 Studying Older Adults' Privacy Decision Making with a Dual-route Privacy Framework

In chapter 3, I show that privacy decisions are, to a large extent, heuristic decisions. Therefore, heuristics should be part of the theoretical framework when studying privacy in addition to the traditional privacy calculus framework. In chapter 4, I incorporate this perspective into my studies: in addition to the traditional privacy calculus framework, I use a heuristic framework to explore older adults' privacy decisions. In the study presented in chapter 4, I show that older adults have a different thinking mechanism compared to younger adults for making privacy decisions. Contradictory to some of the literature, older adults are not reluctant to manage their privacy. Instead, they put effort into making a trade-off between the risks and the benefits of disclosure, even more so than younger adults. Furthermore, in chapter 5, I show that some practices in platform design put older adults at a disadvantage. Framing and defaults are compliance-inducing mechanisms that some platform designers use to maximize compliance. Such mechanisms make older adults more concerned about their privacy and adversely influence their decisions, even more so than younger adults. These studies, however, are incomplete as all of them treat age as a cluster variable. Some of the differences between older and younger adults may be due to the different levels of digital privacy literacy, privacy self-efficacy, or privacy concerns. Therefore in chapter 6, I propose my final study where I measure digital literacy, privacy concerns, and privacy self-efficacy as variables that may justify the effects of age on the decision echo-system. Furthermore, in addition to measuring users' privacy calculus trade-off, I introduce some heuristic manipulations in the decision scenario. This helps us have a deeper understanding of the mechanism through which older and younger adults make their privacy decisions. Figure Figure 1.1 summarizes my framework for studying older adults' privacy decisions. In the next section, I will further discuss this framework based on the literature.

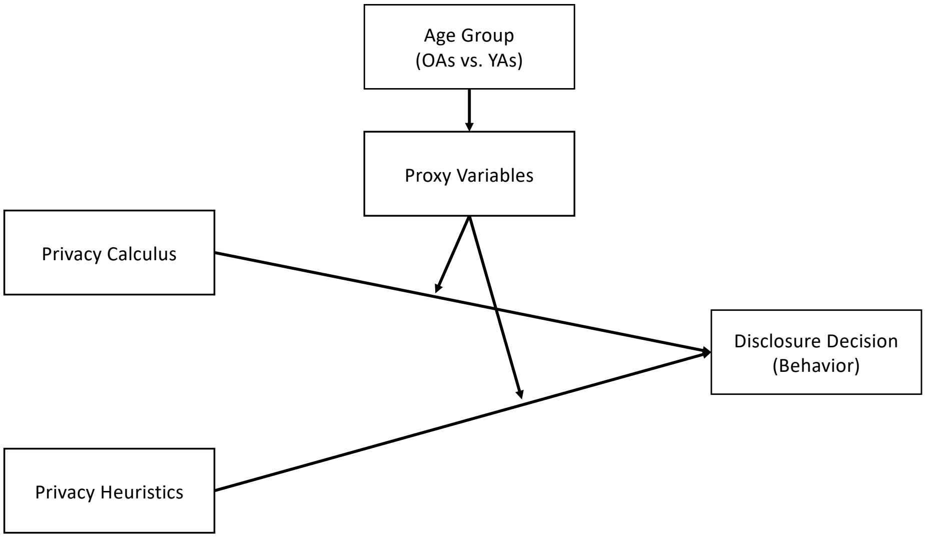


Figure 1.1: A summery of my theoretical framework for studying older adults' privacy decisions

Chapter 2

Background and Theoretical Framework

2.1 Information Disclosure

Information disclosure is a commonly studied outcome variable within privacy research [332, 204, 94, 333, 238] as users' privacy decisions typically involve choosing to withhold or disclose one or more types of personal information. Examples of information disclosure behaviors studied in past privacy research have ranged from whether to share one's financial information to complete an e-commerce transaction [93, 94], one's health data to benefit from a health-app [136], one's location to leverage location-based services [332], or one's personal information to use social networking sites [176].

Disclosing personal information may be advantageous for users, as it gives them access to better or more personalized services that leverage this data [332]. For example, while users might be able to browse an e-map in private mode, they must disclose their location to be able to use GPS features. Likewise, in a messaging app, users can manually enter the recipient's email or phone number, but giving the app access to the user's contacts enables them to select an existing entry, thereby avoiding the hassle of having to type it themselves. The rewards of disclosure, however, come at the cost of diminished privacy: users may worry that their safety could be compromised if their location data is hacked, or they might fear that the messaging app might use their contact list for promotional activities. Thus, users have to decide whether to disclose their information and obtain some gratification or withhold from disclosure and maintain their privacy. In this dissertation, I study different information disclosure scenarios such as revealing personal information to a fictitious financial planning app (see chapter 4), accepting to tag self or a friend in photos on social media (see chapter 3), or giving consent to a website for setting cookies (see chapter 6).

In the following, I review decision-making literature and discuss how individuals make rational or heuristic decisions. Then I start developing a conceptual model for studying the privacy decision-making of older adults.

2.2 Theoretical Frameworks for Studying Privacy Decision Making

2.2.1 Privacy Calculus

When making a choice, the pros and cons of the choice are essential factors that one may consider. Traditionally, decision researchers advocated for the rational choice theory. This theory suggests that individuals can make a rational choice, that is, foresee all aspects of a choice, including the risks and benefits, and make the choice only if the benefits outweigh the risks [274, 267]. This theory is popular in the privacy literature and is referred to as the privacy calculus [83]. Similar to the classical economic perspective, the privacy calculus model argues that individuals trade off the risks of data disclosure against its benefits when deciding whether to share information or not. Consequently, they disclose information only if the benefits out-weight the risks.

The privacy calculus theory is used in numerous studies as the main theoretical framework [161, 93, 176, 94]. It usually involves a trade-off between the positive outcomes of data disclosure versus the negative consequences that may follow. For example, users may disclose their data to receive personalized services [27], post photos on social media for self-expression [159], or share their location for using location-based services [300]. For instance, Krasnova et al. [175] studied self-disclosure in the context of social media using the privacy calculus framework. To assess benefits, they measured the opportunities in social media for relationship maintenance, enjoyment, and self-presentation. To assess disclosure costs, they measured privacy concerns, the perceived likelihood of various privacy violations, and the perceived damage of a potential violation. Overall, they showed that a high perceived benefit and low perceived cost are positively associated with self-disclosure. One of the main rationalistic models in the privacy literature is the APCO (Antecedents, Privacy Concerns, Outcomes) model [277]. APCO results from a broad literature review that studies privacy decisions as byproducts of rational choices. Consequently, the privacy calculus is one of the main actors in this model (See Figure 2.1). The rationale of the APCO model is that some antecedents such as previous experiences or privacy awareness lead to different levels of privacy concerns. Privacy concerns, along with privacy calculus and users' trust, determine users' behavioral reactions (i.e., disclosure or withholding of personal data).

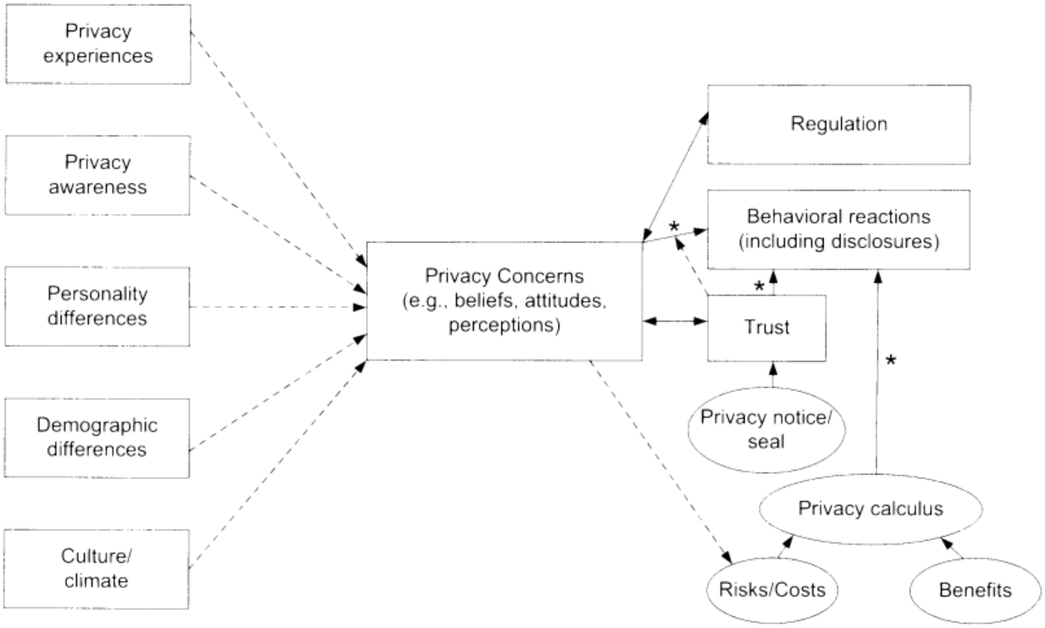


Figure 2.1: The APCO model

2.2.2 Privacy Heuristics

While rational choice theory and privacy calculus made many contributions to the literature, they do not fully align with real-life decisions. There are several reasons that may overshadow a rational privacy decision. Firstly, there are many uncertainties involved in privacy decisions that prevent individuals from having a fair assessment of the potential risks. While the benefits of data disclosure are usually tangible, the potential costs often relate to the perceived uncertainty resulting from sharing personal information [205, 214, 191]. For example, after finalizing an online transaction, individuals may worry that the merchant opportunistically selling consumers' data to others [94]. Furthermore, the collection and usage of personal data do not happen at the same time and place and can happen without users' awareness [4]. This adds to the complexity of privacy decisions. Secondly, privacy decisions are susceptible to malleability and external influences [4]. Platform designers can promote data disclosure by simple changes such as setting the default option on disclosure or using positively framed options (e.g., ”Disclose my information” instead of ”Do not disclose my information”) [146, 179, 150, 7] (See chapter 3). Considering such reasons, many scholars acknowledge the inadequacy of privacy calculus frameworks in justifying privacy decisions [160]. Such factors create a gap between the predictions of the rational choice models (privacy calculus in the scope of privacy) and users' actual behaviors. Indeed, the miss-match between the rational choice and the actual behavior in privacy is so prominent that it is referred to as the privacy paradox [232, 53]. For example, individuals claim to have high levels of privacy concerns, but they freely give up their personal information [75, 32]. Since these empirical observations do not align with the privacy calculus, privacy scholars proposed alternative models to justify users' decisions.

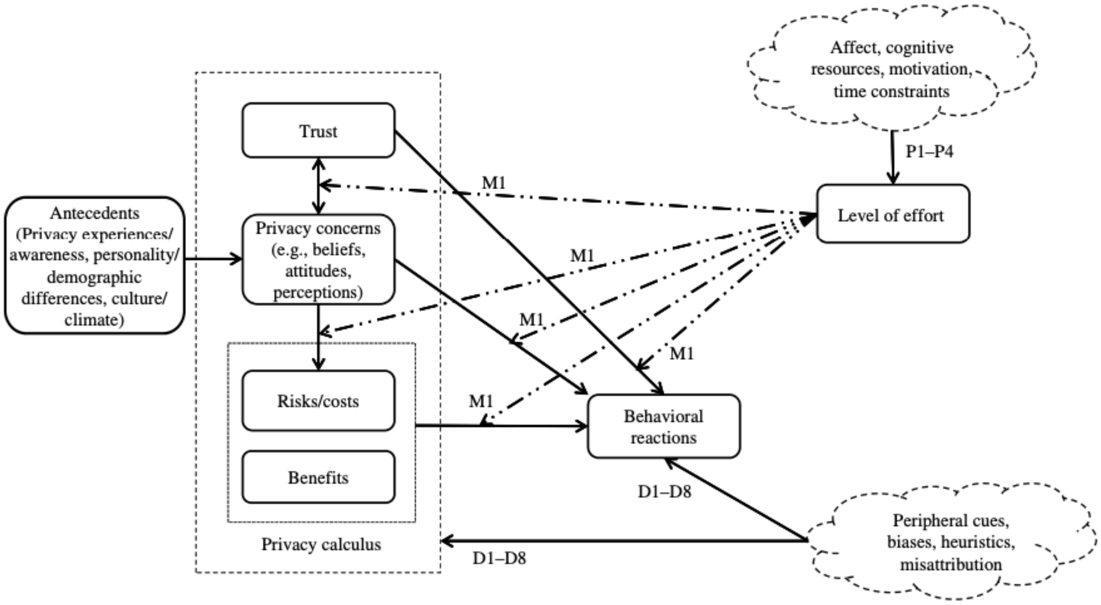

Affect, cognitive resources, motivation, time constraints
P1–P4
Level of effort
Trust
M1
Antecedents (Privacy experiences/ awareness, personality/ demographic differences, culture/ climate)
Privacy concerns (e.g., beliefs, attitudes, perceptions)
M1
M1
M1
Risks/costs
M1
Behavioral reactions
Benefits
D1–D8
Privacy calculus
D1–D8
Peripheral cues, biases, heuristics, misattribution

Figure 2.2: The enhanced APCO model

Scholars developed existing non-heuristic models to accommodate the role of heuristics. A few years later than the original APCO paper, the authors acknowledged that APCO is missing the heuristic aspect of decisions. Consequently, they revisited the APCO model and proposed the enhanced APCO, which also accounts for the role of heuristics such as affect, cognitive resources, and peripheral cues (See Figure 2.2). The higher cloud in the APCO model (P1-P4) includes the cognitive and situational limitations that influence the decision ecosystem. This cloud corresponds to the first set of factors I outlined in the previous paragraph (e.g., uncertainties, lack of knowledge, or motivation about the decision). This cloud justifies why some individuals skip the privacy calculus. For example, lack of motivation will lead users not to spend much effort and overlook the decision. However, the same user could reach a different decision if they have had attended the decision more. The second cloud at the button of the model represents the aspects of the decision that are not necessarily cognitively mediated, which highlights the role of heuristics. A disclosure by default, for example, acts as a heuristic and can have a main effect on the decision outcome [150]. APCO is not the only dual framework model. To leverage the merits of privacy calculus and better account for heuristics, Wang et al. [313] integrated the privacy calculus framework with heuristic shortcuts. They studied self-disclosure on social media using the elaboration likelihood framework. They ascribed the privacy calculus to the central route and other heuristics to the peripheral route. They found that accounting for both the privacy calculus and the heuristics can improve the model. Drawing on these findings, I develop a conceptual framework for studying older adults' privacy decision making which concerns both rational and heuristic accounts (see Figure 2.3). This integrated framework helps us better understand the effects of privacy calculus (i.e., benefits and costs) and heuristic shortcuts (e.g., app trust) on users' information disclosure behavior.

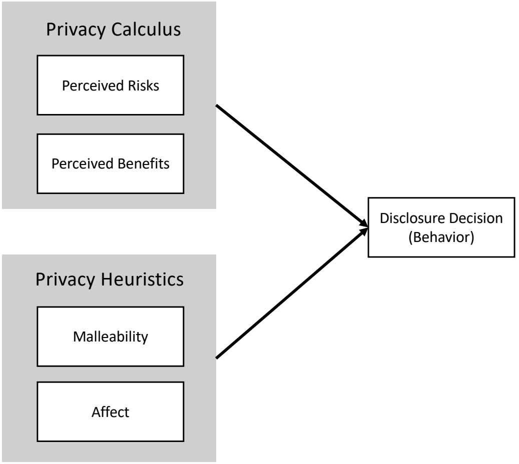


Figure 2.3: Framework 1: A conceptual framework incorporating both privacy calculus framework and heuristic decisions

2.3 Older Adults Population

Older adults—individuals age 65 and above—make up 9% of the world's population [227] and their numbers are growing rapidly. By 2030, the older adult population is projected to reach 1 billion, which will be around 12% of the projected world population [255]. At 15%, the U.S. has an even higher percentage of older adults than the world average [235]. Despite the common perception of older adults as not using technology, a 2009 survey showed that around 40% of them use computers and the Internet [69], and a 2013 report showed that 42% of older adults have smartphones [24]. Internet and technology use are intertwined with privacy concerns for all populations [236, 65]. As 70% of online older adults use it on a daily basis [338], they constitute a major group of Internet users who have privacy concerns [215, 68, 81, 76].

2.4 Older Adults vs. Younger Adults and Privacy

Narratives around technology use and older adults tend to focus on older adults' deficits and difficulties keeping up with younger adults. For instance, Tacken et al. [290] found that many older adults show resistance in adapting to the rapid succession of new technologies [290], and Roger et al.

[259] found that it takes additional time for older adults to learn new technology. Similarly, Czaja et al. [86] uncovered that technology use tends to lead to more anxiety and lower self-efficacy for older adults compared to younger adults. These deficit-based narratives extend into the domain of privacy research as well. Much of the privacy literature examining age-related differences in digital privacy has characterized older adults as having more difficulty than younger adults when managing their digital privacy (e.g., [50, 46, 171, 307, 241]) and generally less likely to protect themselves against privacy risks [294, 336]. For instance, Brandtzæg et al. [50] interviewed Facebook users about privacy features and found that younger adults have an easier time locating and understanding these features compared to older adults. Shujing and Tao's [272] survey-based study concluded that older adults demonstrate low privacy awareness, lack digital literacy, do not pay attention to privacy options, and thus are prone to disclosing too much information online. At the same time, older adults have also been shown to have higher levels of privacy concerns than younger adults [250, 307]. Yet, Van den Broeck et al.[307] found that this heightened privacy concern does not translate to more privacy-protective actions. They studied participants aged 18 to 65 and divided them into three age groups. They found that while the oldest group reported higher privacy concerns, they did not use as many privacy management features as the younger users. To address these heightened privacy concerns and instead of using privacy control features, older adults sometimes avoid the use of digital technologies, such as social media [250]. One possible explanation for the lower use of privacy features of older adults may be that they lack the digital literacy to use such features. Indeed, Park identified a digital divide in technology skills based on age, which was associated with older adults having less privacy control overall [241]. In contrast, Miltgen and Peyrat-Guillard found that younger adults express more positive attitudes around data management and are more confident in their ability to prevent data misuse than older adults [222]. Overall, such findings have led many scholars to conclude that older adults are more vulnerable to security and privacy threats than younger adults[46].

As demonstrated through the findings above, the literature tends to emphasize the deficits of older adults compared to younger adults when it comes to their privacy behaviors, adoption, and use of digital technologies. Yet, focusing on the technology skill deficits of older adults can have detrimental long-term effects by reducing older adults' overall interest and desire to engage with technology in a way that benefits them [221]. While older-adult-friendly designs may account for age-related changes in motor control, perceptual function, and cognitive ability, many technologies do not tailor their services to older adult populations [105, 258, 110]. Indeed, Frik et al.[110] urge designers and developers to specifically consider the older adult population when developing new products. They identify common misconceptions among older adults (e.g., if they have nothing to hide, they should not be worried about privacy) and argue that product designers should consider these beliefs in order to design effective systems that can empower older adults. Thus, the problems associated with older adults' technology use may instead be due to the deficits in the design of technologies, which often cater to the needs of younger adults.

Some scholars are moving away from painting older adults as technology Luddites. For example, Knowles and Hanson [171] took a strength-based approach by interviewing older adults to understand their resistance against technology adoption. They found that older adults had legitimate concerns regarding the use of digital technologies, and the risks associated with use often outweighed the benefits. As such, these researchers chose to emphasize the "wisdom" older adults demonstrated in their decision-making process not to engage with technology. Hoofnagle et al. [134] showed that younger and older adults are not different in terms of attention to privacy policies. They also asked participants some comprehensive questions to assess their online privacy knowledge. Overall, while only 12% of younger adults answered at least 3 out of 5 of the questions correctly, 25% of older adults performed that well. Indeed, older adults may not underestimate privacy risks [135], and their low technology use rate can be due to an informed privacy decision (i.e., non-use due to costs outweighing benefits) rather than an inability to learn [171].

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

The psychological literature confirms that older and younger adults exhibit fundamental behavioral differences in their patterns of decision-making, including differences in risk preference and reliance on goal-driven strategies [327]. The relationship between aging and decision-making has been examined in several contexts. In risky choice contexts, older adults tend to be less risk-taking overall compared to younger adults [152]. However, older adults are often more willing to take risks to avoid a loss than obtaining a gain compared to younger adults, although this relationship can vary depending on the magnitude of what is at stake [43, 60]. Furthermore, the age-related positivity effect also affects decision-making strategies. This effect refers to a tendency for older adults to have heightened attention or give more weight to positive information or stimuli during the decision-making process and less weight or attention to negative information [208]. Thus, if negative information is not completely salient in a given decision scenario, older adults may be more attentive to the positive aspects of a decision than negative aspects. These findings suggest that studies should account for the fact that the decision process is different for older and younger adults.

Drawing on this literature, elements of rational or heuristic decisions may play different roles in users' behavioral decisions (see chapter 4). Therefore, in the second conceptual model, I consider the effect of privacy calculus and privacy heuristics being moderated by the age groups (see Figure 2.4).

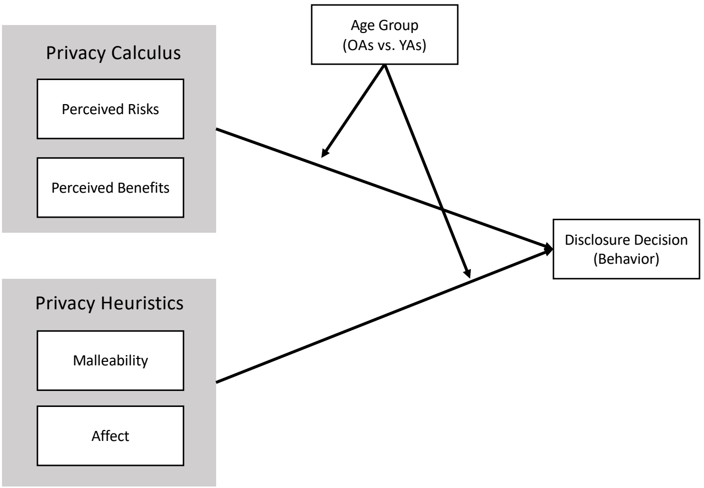


Figure 2.4: Framework 2: A conceptual framework for studying privacy decisions while accounting for age groups

However, as discussed in chapter 1, the difference between young and older adults is arguably not only age. Instead, there are more fundamental variables that may set these two populations apart. The difference in older and younger adults' decision processes may be due to such variables rather than the age group. I will outline such variables in the following section.

2.6 Disentangling Age

Many scholars study older and younger adults' decisions by separating the two populations in terms of age groups. They use age as a binary (older vs. younger) or as a continuous variable. However, these studies fail to explicitly acknowledge that age may be a *proxy* rather than the actual variable contributing to the differences between the age groups of interest. In this section, I propose relevant constructs that may replace age by explaining the models better.

2.6.1 Digital Literacy

Digital literacy involves individuals' competencies in the use of digital technologies [40]. A digitally literate individual can use technology effectively as means to reach particular personal and professional goals [335]. The literature cites lack of digital literacy as one of the barriers towards technology use, and adoption [55, 228, 335].

In the privacy literature, digital literacy is noted as one of the factors relating to online privacy decisions [325, 241, 124]. The general argument in the literature is that a high digital literacy may reduce the likelihood of privacy violations. Research suggests that those who have higher digital skills are more likely to exercises control over their online privacy [241]. This may be justified by more heightened privacy awareness among digitally literate individuals [241]. The lack of digital literacy can be even more problematic in more complex technologies with vast data collection affordances. Wearables devices, for example, follow pervasive data collection mechanisms. These devices are intended to be worn 24 hours a day, collecting different types of sensitive data such as health, and location [242]. Users may be unaware of these data collection practices [224], or not be able to exercise control due to the complex ecosystem in such devices [124]. These new and complex technologies can reinforce the adverse effects of low digital literacy on online privacy decisions.

The digital divide between the younger and older adults worsens the situation for the more aging population. The literature suggests that there is a digital divide between young and older adults, with older adults having lower levels of digital literacy [328]. This digital divide creates an unfortunate scenario in which older users are more likely to be the victims of identity theft or related online crimes [241]. Therefore, it is necessary to account for digital literacy in studies concerning age and privacy decisions. Chapter 6 will discuss the related work in digital literacy further.

2.6.2 Privacy Self-efficacy

One's belief about their capabilities of successfully performing a task is regarded as Self-efficacy [35, 33]. A strong sense of efficacy can drive human behavior and increase human accomplishments, and their mental well-being [35]. This makes self-efficacy a good predictor of whether or not one performs a task or how well the performance would be [128]. In the realm of technology, for example, self-efficacy can reduce some barriers of technology adoption [252]. Therefore, individuals with higher levels of computer self-efficacy are more likely to adopt information systems [145].

Privacy self-efficacy is one's confidence in protecting their privacy [187] and can influence privacy decisions [73, 72, 130, 21]. Individuals with higher self-efficacy can better align their privacy attitudes with their behaviors [73]. Self-efficacy is the subject of studies concerning age and is expected to be different across older and younger adults [178, 112]. Zeissing et al. [336] for example, hypothesized that older adults have lower privacy self-efficacy compared to their younger counterparts. However, they found the opposite and concluded that their measure of privacy self-efficacy reflects users' confidence in their protection abilities, which is different from the comprehensiveness and completeness of such abilities. They called for future research to study this construct further. Due to this research gap, the importance of this construct in the privacy literature, and its relevance to age, I add privacy self-efficacy to the framework as a hidden variable. Chapter 6 will discuss the related work in privacy self-efficacy further.

2.6.3 Privacy Concerns

Privacy concerns are among the most commonly studied variables in the privacy literature [94]. Individuals feel worried about the loss of their privacy, especially if they notice an unwarranted data collection or use [312, 66]. Privacy concerns is an antecedent to several behavior-related outcomes such as willingness to disclose personal information for a personalized service [70], carrying out online transactions [94], self disclosure in social media [122], and giving different access permissions to the mobile applications [90].

While many scholars argue that younger adults are less concerned than older adults, few studies actually measured and compared older and young adults' levels of concerns [134]. There is no consensus among studies that measured privacy concerns for both age groups. Van den Broeck et al. [307] for example, found that older users have greater privacy concerns. However, paradoxically they are less likely to utilize privacy features. Hoofnagle et al. [134] studied young and older adults' concerns and did not find significant differences in their concerns. Studying privacy concerns across both age groups is necessary to answer some of the remaining research questions in the field.

Based on these discussions, I outline the third conceptual model in Figure 2.5, where the moderating effect of age groups is being mediated by more fundamental constructs. I will explore this model further in chapter 4.

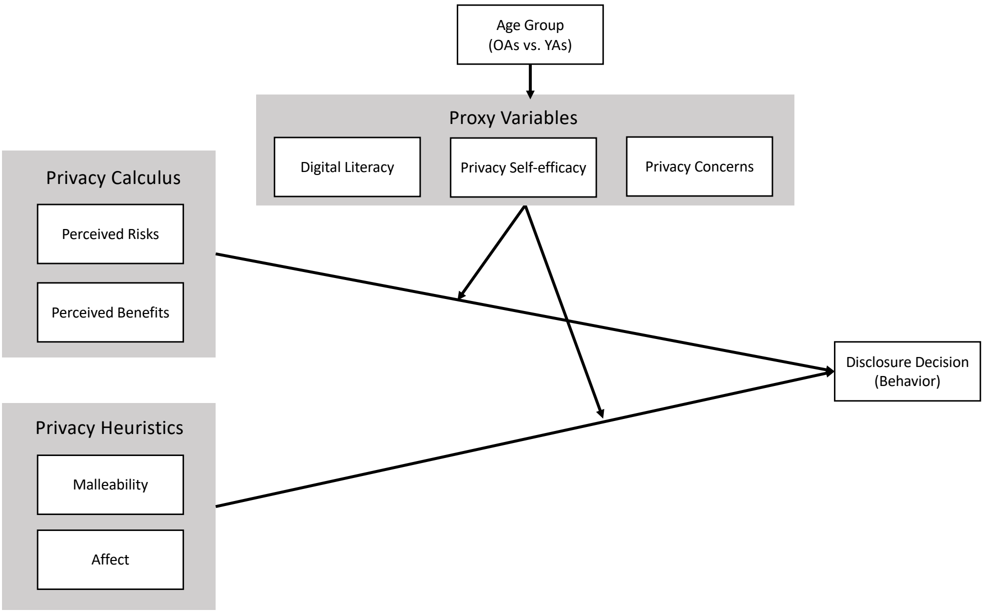


Figure 2.5: Framework 3: A conceptual framework for studying older adults privacy decisions. This model accommodates two different thinking mechanisms: a heuristic account and an economic, calculus-driven account. Furthermore, the hidden variables (e.g., digital literacy, privacy self-efficacy, and privacy concerns) are incorporated as moderators.

Chapter 3

Malleable Privacy Decisions

In chapter 2, I raised a case for heuristic frameworks to be used in privacy studies. While I presented privacy calculus as a rationalistic framework that justifies a significant portion of privacy decisions, I also discussed how privacy calculus leaves a substantial portion of decisions unexplained. I argued that privacy decisions are not necessarily a result of a rational decision. The study presented in this chapter is an empirical showcase of such situations, where individuals make choices based on heuristics. In this study, I use a common scenario where platforms promote heuristic decisions: consent mechanisms. Since heuristic decisions are not a result of rational deliberation, companies use design elements to encourage heuristic decisions to nudge their clients to comply with disclosure requests mindlessly. I consider this compliance ”mindless” because it relies merely on randomized experimental manipulations rather than a rational privacy calculus.

Companies can easily avoid fines for privacy violations if they obtain informed user consent. In this context, consent refers to a freely given, specific, informed, and unambiguous indication that a user has agreed to allow a company to process the user’s personal data [326]. Companies have a major incentive to discourage users from extensively deliberating about privacy during the consent procedure since researchers have found that privacy concerns decrease users’ intention to use online services [243]. To this end, some technology companies and application developers have resorted to mechanisms that promote ”mindlessness”—a state in which users behave like programmed automatons [181] who do not consciously scrutinize their options [256] or generally remain vigilant about their decisions [287, 298]. By obtaining mindless compliance, technology companies not only fulfill their legal requirements but also make it unlikely that users will become alert in terms of privacy, which makes users more likely to comply with their request [150, 245]. These mechanisms rely on the fact that individuals tend to favor compliance when responding to another entity's explicit request [115]).

To induce mindless user compliance and, thus, swiftly obtain informed consent, companies commonly use framing and default effects. Framing effects refer to irrational influences that an option's presentation has on a user's choice[157, 303] , and default effects refer to irrational influences that an option's pre-selection has on a user's choice [264]. I consider the compliance that framing and default effects induce "mindless compliance" because it merely relies on the framing type or default settings rather than a deliberate tradeoff between the risks and benefits of complying. For example, regarding privacy-related compliance, Johnson et al. [146] and Lai and Hui [179] independently found framing and default effects to have a significant impact on users' privacy decisions. Johnson et al. [146] studied participants in a health survey and measured their willingness to receive notifications about other health surveys, while Lai and Hui [179] studied participants in a website evaluation study and measured their willingness to receive a newsletter from the website. The researchers in both studies presented the decision as a checkbox with a label. They manipulated the framing via the wording on the label: they used "please send me newsletters" as the positive framing and "please do not send me newsletters" as the negative framing. For the default condition, they manipulated both the framing and the checkbox's status (i.e., pre-checked or not): in the positive default condition, when users clicked the "next" button without any changes, they accepted the request; in the negative default condition, when users clicked "next", they would reject it. Both studies found that framing and defaults had a separate and additive effect on users' decisions and that a positive default and/or framing led to higher levels of disclosure than negative defaults and/or framing. These results suggest that companies can use framing and default effects to induce mindless privacy compliance by manipulating user decisions in their own favor.

In order to obtain informed consent, companies often choose to add justifications for the different options they present to users. Social scientists have long established the causal effect that different types of justifications have on compliance in terms of norms [28]. For example, Cialdini, Reno, and Kallgren [80] found that people are less likely to litter in an environment with a single piece of litter than in an environment with no litter at all because the single piece of litter will remind them about the injunctive social norm that "one ought not to litter". However, people are more likely to litter in a fully littered environment because the descriptive social norm that "people do litter here" has more salience than the injunctive social norm, which causes a herding effect [26, 137]. Researchers have argued that default and framing effects occur because they represent an injunctive social norm [213, 271]. Therefore, analogous to Cialdini et al.'s [80] findings, one could argue that a justification that presents a salient descriptive social norm could potentially override this injunctive social norm with a herding effect. However, researchers have not tested this analogy and, thus, the interplay between defaults/framing and normative justifications. These interacting effects, however, commonly occur when users make decisions about privacy consent online, and we need to explore them to guide user and policy decision making. In this chapter, I fill this gap by covering social norm-based justifications, but, for comparison, I also add another common type of justification: rationale-based justifications.

In their groundbreaking field experiment on rationale-based justifications, Langer, Blank, and Chanowitz [182] showed that not only plausible rationalizations (i.e., "Excuse me, may I use the Xerox machine because I'm in a rush") but also placebic rationalizations (i.e., "Excuse me, may I use the Xerox machine because I have to make copies") can help generate compliance (allowing the requester to cut in line for a copy machine) for small favors (five copies). For larger favors (20 copies), however, rationale-based justifications only result in compliance when they are plausible and not placebic. In this and the following studies, it remained unclear how the absence or presence of such compliance-inducing justifications interacts with framing and default effects on compliance. Importantly, researchers have only studied the effect with placebic justifications–in a justification-assisted privacy decision setting, such justifications are more likely to be incongruent rather than immaterial with respect to the prevailing framing/default. Moreover, researchers have only studied this effect with positive defaults—it remains unclear whether it can also cause compliance with a negative default (and, indeed, with positive and negative framing). I fill these two gaps in this chapter.

In particular, I address the following research question (RQ):

RQ: Do justifications override the mindless compliance effects of defaults and framing as Cialdini et al. [80] suggest, do they exacerbate mindless compliance as Langer et al. [182] suggest, or does this effect depend on the justification type?

To address this research question, I conducted an elaborate experiment in the context of a self-developed Facebook photo-tagging application. Researchers have often criticized default and framing studies for using hypothetical scenarios. Because such hypothetical scenarios lack real risks and benefits, they might not motivate users to elaborate on their preferences in the first place and, hence, exacerbate default and framing effects. In a privacy context, relying on such results can be more misleading since individuals make privacy decisions ad hoc under a situation's particular requirements [186]. The privacy decisions that I investigate involve consenting to (automatically) tagging oneself in one's friends' Facebook photos and tagging one's friends in one's own Facebook photos. To ensure ecological validity, users had to log in to their Facebook account through Facebook's official log-in buttons and, hence, perceived that their decisions had real risks and benefits.

The experiment discussed in this chapter comprises a 2 x 2 x 5 design. I first introduce compliance biases through established default and framing conditions. To address the impact of justifications, this study compares two types of justifications: one with a rationale (information about the possible positive or negative consequences of using the automatic photo-tagging system) and one with a descriptive social norm (fictive information on the percentage of study participants who use the automatic photo-tagging system) against a baseline of no justification. Each justification had a positive (pro-tagging) and negative (anti-tagging) valence condition.

In one aspect, this study uniquely differs from previous studies on justifications: while researchers have studied normative [80] and rationale-based [182] justifications in face-to-face scenarios, I used computer-mediated manipulations. My findings suggest that the compliance-inducing effects of defaults and framing persist in an ecologically valid privacy decision-making setting. Furthermore, I replicate Langer et al.'s [182] finding on the compliance-inducing effects of rationale-based justifications. The results further expand those findings by showing that even a conflicting justification that cautions users not to use the tagging application can increase their compliance with the positive default and that the effect also works to increase compliance with the negative default. Finally, I discuss the effect that normative justifications have on users' privacy decision making. Overall, the results demonstrate the potency of justifications in exacerbating mindless compliant behavior during privacy decision making.

This chapter proceeds as follows: in section 3.1, I discuss the literature and theoretical background. In section 3.2, I describe the experimental setup. In section 3.3, I present the results. In section 3.4, I discuss the results. In section 3.5, I discuss the study's limitations and potential future research directions. Finally, in section 3.6, I conclude the chapter.

3.1 Theoretical Background and Research Framework

In this section, I first briefly cover related work regarding compliance and privacy decisions on Facebook. Subsequently, I describe how framing and default effects induce compliance and discuss the potential moderating role of justifications.

3.1.1 Collective Privacy Management on Facebook

Users sometimes overshare information on social media [11], which can have unintended consequences [260]. Therefore, Facebook users employ various strategies to manage their interpersonal boundaries: they manage their relational boundaries (e.g., friending and unfriending), territorial boundaries (e.g., untagging or deleting unwanted posts), network boundaries (e.g., hiding their friends list), and interactional boundaries (e.g., blocking other users or hiding one's online status) [237, 323]. Pempek, Yermolayeva, and Calvert [244] found posting and viewing photos among the top three reasons why college students use Facebook. A particularly interesting part of users' privacy-management practices involves their uploaded photos because they may depict other Facebook users (including their friends) as well. Facebook has a mechanism to explicitly indicate whether a photo contains a person called "tagging". Notably, Facebook users may "tag" not only themselves but also others in their own photos, and they can also tag themselves in others' photos . The photo-tagging concept exemplifies "collective privacy management" [74, 143] since it collectively engages users in managing privacy-related information that impacts multiple individuals [173, 249]. Research has shown tagging other people in one's photos to be a contentious issue when a user has risqué or compromising photos of their friends in which they would rather not be tagged [42, 125, 286]. At the same time, though, photo tagging can have beneficial effects: it builds social capital, increases group cohesion, and allows one to express one's identity [125, 216, 262, 286]. The tendency to tag photos also relates to users' perceptions about the tagging feature's ease of use[174], which means that a system that automatically tags photos [284] can have substantial benefits.

I focus on photo tagging on Facebook in this study because it provides a realistic use case for studying compliance. To a large extent, users' preexisting personal privacy preferences govern their personal privacy decisions. In contrast, the interdependent nature of photo tagging decisions likely makes them more amenable to external influences, such as the perceived social norms among a user's friends. As such, framing, defaults, and the proposed moderators have a substantial opportunity to influence user compliance.

3.1.2 Compliance

As I mention at the beginning of this chapter, online companies that process their users' personal data must obtain informed user consent to allow them to do so. In this study's context, users express consent through the compliance with the request to (not) automatically tag photos. In this section, I cover two perspectives on compliance: the normative perspective and the mindless compliance perspective. Subsequently, I discuss the compliance-inducing effects of defaults and framing and how justifications can influence this compliance.

3.1.2.1 Compliance to Norms

Findings in social psychology suggest that people do consider different norms such as personal, social, or situational norms, each of which can either be injunctive or descriptive [78, 79]. These different norms can induce compliance, whether the norm be what the majority of people do (descriptive) or what others find appropriate or acceptable (injunctive) [269]. Researchers generally agree that, in any given setting, these different norms compete for a person's attention [131]. Cialdini et al.'s [79] norm salience theory suggests that, in the presence of competing norms, people are more likely to comply with the most salient norm. This norm has to be focal to influence people's behavior [79, 80, 158, 253].

For example, Cialdini et al. [80] found that people are less likely to litter in an environment with a single piece of litter than in an environment with no litter at all because, they argue, the single piece of litter will make the injunctive social norm that "one ought not to litter" focal. However, they also showed that people are more likely to litter in a fully littered environment because, they argue, the descriptive social norm that "people do litter here" has more salience in a littered environment than the injunctive social norm. Interestingly, the injunctive social norm becomes focal again when someone makes an effort to clean the littered environment, and people's tendency to litter decreases accordingly [79, 80].

In the privacy context, the IS literature has shown that both descriptive and injunctive norms can predict privacy behaviors. For example, Ju et al. [154] showed that users who receive more information about a product's benefits (high injunctive norm) are more likely to grant permissions to a mobile app than users who receive less information about its benefits (low injunctive norm).

They also showed that participants who learn others share more data than what they do (positive descriptive norm) are likely to grant more permissions to the mobile app.

3.1.2.2 Mindless Compliance

An alternative view on compliance posits that it mostly occurs outside a user's mindful thought processes. An extensive body of research has investigated drivers for such "mindless compliance". Milgram's [219] experiments most prominently sparked the discussion on the extent to which commands from an authoritative figure can move people to engage in harmful or potentially even lethal behaviors. Even though researchers have discounted the validity of Milgram's experiments today, Milgram motivated a substantial body of research that investigated compliance-inducing strategies that people can use without the special authority a researcher may enjoy (e.g., salespeople, charities, friends). Companies generally induce compliance through emotional and/or rational appeals.

In the privacy domain, mindless compliance to a disclosure request can adversely affect both organizations and users. For example, in the infamous Cambridge Analytica case, defaults influenced users' decisions to share personal information with rather unfavorable consequences. Facebook lost not only billions of dollars in its net value [257] but also users' trust [318]. In fact, many users said that they did not remember giving permissions to the app that Cambridge Analytica used, which further indicates their mindless compliance [63].

3.1.3 Inducing Compliance with Framing and Default Effects

In the study presented in this chapter, I examine how framing and defaults affect users' compliance to privacy requests. Thaler and Sunstein [296] have noted that one can use framing and default effects to nudge users in the desired direction. When applied to decisions such as organ donation, healthy eating habits, or energy saving, this "soft paternalistic" approach can lead to great social benefits. Likewise, in the privacy literature, recent work has employed nudges as a means to protect social network users' privacy [1, 30, 138, 314]. However, one can question the ethical validity of nudges (even if they benefit society) since they might not reflect individuals' true preferences and, thus, can be perceived as manipulative. Furthermore, some researchers argue that defaults cause behavioral or cognitive biases, which threaten consumer autonomy [278, 280]. They consider default and framing effects harmful because, among other reasons, one often cannot avoid them:

many (privacy) decisions must have a certain default setting, and a neutral frame does not exist [296].

To deal with the default effect, one can set the default option to the choices most people are comfortable with (Johnson et al. [150]). However, Smith, Goldstein, and Johnson [278] have noted that, in most consumer decisions, the desired outcome may differ for different individuals depending on their individual preferences. This criticism applies in particular to privacy decisions, which tend to vary extensively [319]. Thus, one cannot easily circumvent the fact that framing and default effects may move users away from their "true preferences" [144], and such a deviation between users' true and selected preferences will likely backfire and cause dissatisfaction, especially on social networks [315]. Thus, in this chapter, I focus on the compliance-inducing effects of defaults and framing.

3.1.3.1 Framing Effects

One can also explain framing effects as normative effects. Sher and McKenzie [271] demonstrate that people are more likely to use a positive frame when they have a positive attitude towards something and a negative frame when they have a negative attitude towards it. Conversely, a decision maker may interpret the positive or negative framing of a decision as representing the positive or negative attitude the requester has towards the decision [271]. As such, the framing serves as a clue that relates to injunctive social norms [79, 80, 158]. Injunctive social norms describe what an individual ought to do in a certain situation (as opposed to descriptive social norms, which describe what people do). Thus, a positive frame suggests an injunctive norm that supports an action, while a negative frame suggests an injunctive norm against an action.

In this study, attribute framing manifests in whether users have the option to apply the automated tagging procedure or rather the option not to apply the automated tagging procedure. Based on existing evidence [146, 179, 123], different frames will induce different levels of compliance. Thus, I hypothesize that:

H1:*A positively framed tagging request results in higher tagging rates compared to a negatively framed request.*

3.1.3.2 Default Effects

The default option refers to the option that a decision maker will receive if they do nothing. Research shows that people are more likely to accept an option if that option is selected by default. In this regard, researchers have found a positive default to increase pension saving [202], insurance signup rates [149], and organ donation [148]. Dinner, Johnson, Goldstein, and Liu [96] present the effort of choosing the default as a potential cause for the default effect either in terms of physical effort (changing the default requires action; see [264]; [297]) or mental effort (changing the default requires making a tradeoff that takes time and cognitive effort (see [303]).

Another explanation for the default effect posits that, like framing, individuals perceive defaults as an injunctive social norm (i.e., an implicit endorsement from the requester), which nudges them towards accepting the default option [96, 213].

In this study on Facebook photo tagging, the default setting manifests in whether the Facebook will apply or rather not apply the automated tagging procedure if the user simply does not change the current setting. A pre-checked checkbox in the positive framing condition or an empty checkbox in the negative framing condition translates into the user accepting the auto-tagger by default. Conversely, an empty checkbox in the positive framing condition or a pre-checked checkbox in the negative framing condition translates into the user rejecting the auto-tagger by default. Based on existing evidence and given that different default conditions can induce different levels of compliance [146, 179], I hypothesize that:

H2:*An accept-by-default tagging request results in higher tagging rates compared to a reject-by-default tagging request.*

3.1.4 Justifications as Moderators for Mindless Compliance

During privacy consent decisions, companies often provide additional information about the different options they present to users. Optimistic advocates for the individuals' ability to make informed decisions might propose that educating users with additional information about the choice can mitigate mindless compliance-inducing mechanisms [119, 188]. For example, Cialdini et al. [80] show that a salient descriptive social norm can override an injunctive social norm. Hence, a normative justification (e.g., "xx% of people engage in behavior Y") might be able to weaken the effects of defaults and framing. Likewise, descriptive justifications that inform users about a product's quality from other consumers' viewpoint (cf.[99]) can trigger social proofing [77] or herding [26, 137], which can similarly weaken their effects.

However, this argument suggests that a more salient and contradicting normative or descriptive justification can start a mindful process to mitigate the compliance-inducing effects of an existing norm. In contrast, Langer et al. [182] suggested that justifications may in fact make compliance less mindful and, thereby, exacerbate the compliance-inducing effects of defaults and framing. In their study, an experimenter asked participants for a favor. In one condition, the experimenter did not provide any justification for the request, but, in the two other conditions, the experimenter provided either a placebic (”May I use the Xerox machine because I have to make copies?”) or a plausible (”May I use the Xerox machine because I'm in a rush?”) justification. The authors found that, for small favors , the plausible and placebic justifications worked equally well, and both resulted in more people mindlessly complying with the request than the no-justification condition. The authors explained these results by arguing that participants expect the interaction to be mindful and, hence, expect a justification to be plausible rather than placebic. Rather than actively processing the placebic justification, they simply assume that it is plausible. From this perspective, one could argue that justifications (any justification regardless of whether they are congruent or incongruent with the decision's prevailing framing/default) would likely exacerbate rather than mitigate the mindless compliance that the default or framing induces.

To resolve this theoretical contradiction, in this study, I test the effects of two common types of justifications on mindless compliance: descriptive normative justifications and rationale-based (injunctive) justifications. I then identify how positive (pro-compliance) and negative (anti-compliance) versions of these two types of justifications can influence the compliance that framing and defaults induce. In addition, I compare a justification's absence versus its presence.

3.1.4.1 Descriptive Normative Justifications

Descriptive normative justifications (e.g., ”xx% of people engage in behavior Y”) provide a social nudge for individuals to either engage in (with a high percentage) or refrain from (with a low percentage) the target behavior. Individuals could perceive such normative justifications—especially the high-percentage ones—as social proofing that confirms the behavior's validity [77], which could induce a herding effect [26, 137]. Thus, they can increase the target behavior accordingly.

Given that both framing and default effects introduce an injunctive social norm (i.e., what people ought to do) [213, 271], Cialdini et al. [80, 79] would propose that a sufficiently salient justification that presents a conflicting descriptive social norm (i.e., what people actually do) can reduce or even eradicate the mindless compliance that framing and defaults induce.

However, this argument presumes that people actually attend to and process the justification messages. Langer et al.'s [182] work on mindless compliance showed that people do not necessarily do so; if they consider the target behavior a small favor, they may possibly consider a justification's mere presence a good reason for the request (without actually processing the justification) and, thus, comply with it. This logic suggests that the descriptive normative justification exacerbates the compliance-inducing effects of defaults and framing. To acknowledge these competing assumptions, I hypothesize that:

H3: *Descriptive normative justifications moderate the effect that framing and defaults have on mindless compliance; that is, a descriptive normative justification can strengthen or weaken the effect that framing and defaults have on mindless compliance.*

3.1.4.2 Rationale-based Justifications

Rationale-based justifications (e.g., describing the positive or negative consequences of engaging in a certain behavior) can nudge users' disclosure by providing a rationalization for choosing one option. As such, one would expect that positive rationale-based justifications increase the target behavior, while negative rationale-based justifications decrease it.

Moreover, rationale-based justifications might constitute an injunctive social norm that provides either an endorsement or caution about the target behavior. According to Cialdini et al. [80], this justification can reduce the mindless compliance that framing and defaults induce provided that it has sufficient salience.

On the contrary, these justifications can serve as rationalization for users (e.g., the app might be good if others also use it) in the sense of Langer et al.'s [182] work on mindless compliance. In this case, users would not mentally process the rationale-based justifications, which would simply increase their tendency to comply with the request. Given these competing assumptions, I hypothesize that:

H4: *Rationale-based justifications moderate the effect that framing and defaults have on mindless compliance; that is, a rationale-based justification can strengthen or weaken the effect that framing and defaults have on mindless compliance.*

Langer et al. [182] conducted their study with in-person conversations; however, the liter-

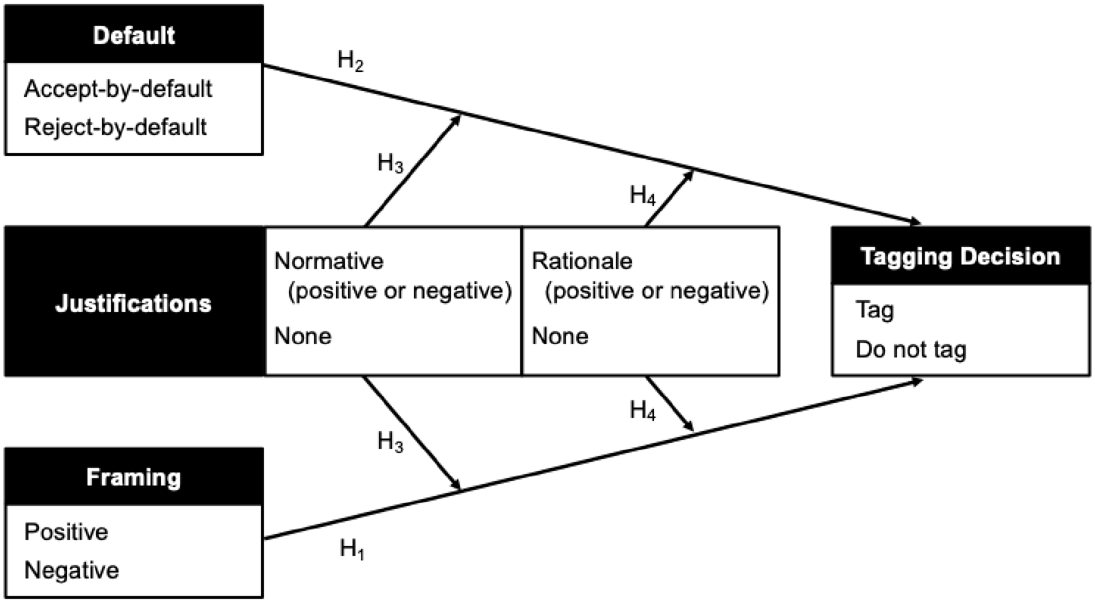


Figure 3.1: Research Model for the Moderating Effects of Justifications on Mindless Compliance Induced by Framing and Default Privacy Settings
Model

ature does not show how users in a tagging application—or any online scenario—would perceive a similar request as the ones they asked. Moreover, Langer et al.'s [182] experimental scenario (asking for permission to cut in line) does not have a natural complement in terms of default or framing. Their request compares to a positively framed accept-by-default scenario; a negatively framed scenario would be similar to asking for permission not to cut in line (i.e., "Excuse me, may I not use Xerox machine?"—a rather uncommon request). On the contrary, privacy decision making scenarios commonly use negative framing. Research suggests that users perceive negatively framed and/or reject-by-default decisions as expressing the requester's negative opinion about the target behavior; therefore, users can perceive them as requests not to engage in the target behavior [213, 271]. In this case, extrapolating Langer et al.'s [182] findings, one would expect that rationale-based justifications can further exacerbate the negative default and/or framing effect as well (i.e., further reducing disclosure).

Finally, whereas Langer et al. [182] compared a plausible justification against a placebic justification, I opt to compare a plausible justification with a positive valence (arguing the reasons for the action) against a similar justification with a negative valence (arguing the reasons against the action). If people truly do not process the justification as Langer et al.'s theory suggests, then my comparison may work just as well, but researchers have not tested it until now.

Figure 3.1 summarizes the experimental model. In section 3.2, I discuss the experimental environment and how I operationalized the research questions.

3.2 Method

To investigate the privacy-related compliance with framing and defaults and the potential moderating effect that justifications have on this compliance, I conducted an elaborate experiment in the context of a self-developed Facebook photo-tagging application. Given the popularity of photo sharing on Facebook, with this study design, I could simulate a realistic privacy scenario that people with a broad range of socio-demographic characteristics could relate to.

3.2.1 Participants

I recruited 50 participants for a pilot study and 1084 participants for the actual study through online platforms. Participants were paid US$1.30 for their participation. The designed platform required users to have an active Facebook account with at least ten friends to participate in the study. On average, the participants had 427 Facebook friends.

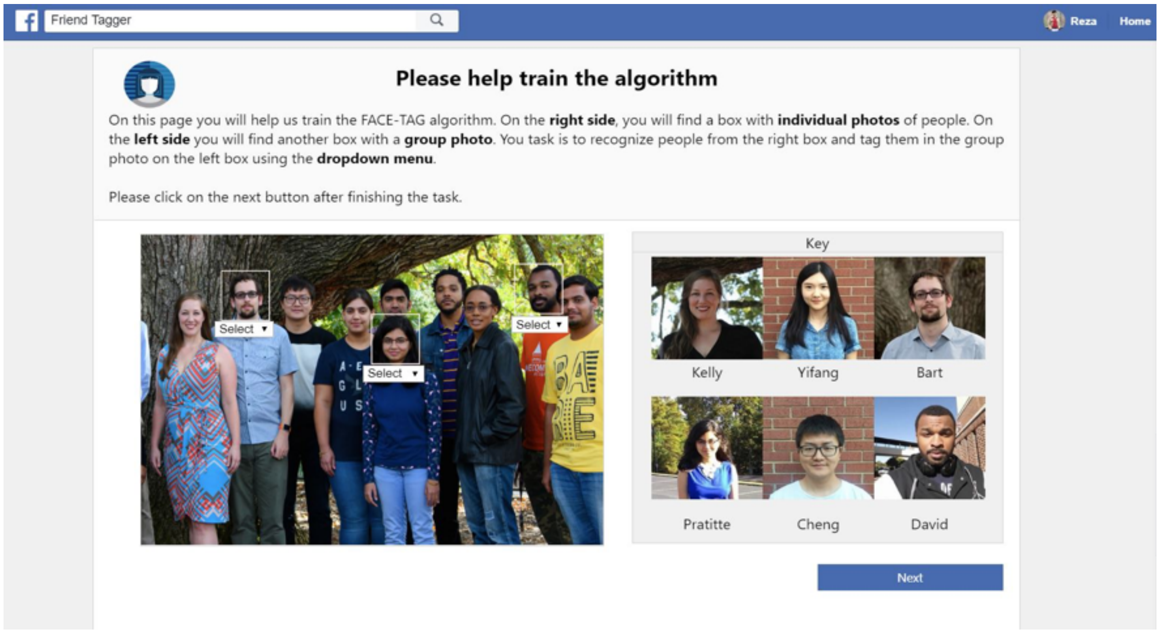
3.2.2 Experimental Setup

3.2.2.1 Pre-questionnaire

I told participants that our team was developing a Face-detection algorithm for a Facebook application that can automatically tag people in photos. I first asked them questions about their Facebook usage such as the time they spent on Facebook and how frequently they used it. I then redirected them to a page where the app asked them to log in to Facebook and use the application.

3.2.2.2 Facebook Application

I asked participants to log in to their Facebook account by giving basic profile and friend list permissions to the app. In the app, as a first task, I asked participants to test the readability of a note that said: "This is a free application being developed by university researchers that can automatically tag the users or users' friends with high accuracy. Should the app make a mistake, users can still



Please help train the algorithm

On this page you will help us train the FACE-TAG algorithm. On the **right side**, you will find a box with **individual photos** of people. On the **left side** you will find another box with a **group photo**. You task is to recognize people from the right box and tag them in the group photo on the left box using the **dropdown menu**.

Please click on the next button after finishing the task.

Figure 3.2: The ”Training” Phase

remove the tags.”. A short survey asked comprehension questions about this explanation, and I asked anyone who did not answer the questions correctly to read the note again. With this procedure, I could make sure that every user understood the benefits and consequences of using the application in order to make the eventual decision’s value proposition (see below) unambiguously clear and equal for all participants.

Participants then entered the study’s ”training” where they tagged the people in four researcher-provided photos based on a key I provided to them on the screen. Figure 3.2 shows the first training page.

After four training pages, participants entered the study’s ”correction” phase. In this phase, the app displayed photos that the algorithm had ostensibly tagged and asked participants to correct any mistakes. I made sure that participants would have to make no corrections at all: all the tags in these photos were correct. This phase demonstrated to participants the algorithm’s reliability so that they would not have to be worried about algorithmic accuracy in their subsequent decision.

Next, participants entered the study’s ”decision” phase where the app told them: ”Before we continue with the final part of the study, we want to give you the opportunity to actually use our app. Please choose from the options below. Note that whatever you choose will not affect your compensation.”. At this point, I presented participants with the opportunity to use the autotagging procedure themselves—a question that was manipulated in terms of default, framing, and justification (see Section 3.2). As the dependent variable, I measured the outcome of the tagging decision (tagging vs. no tagging).

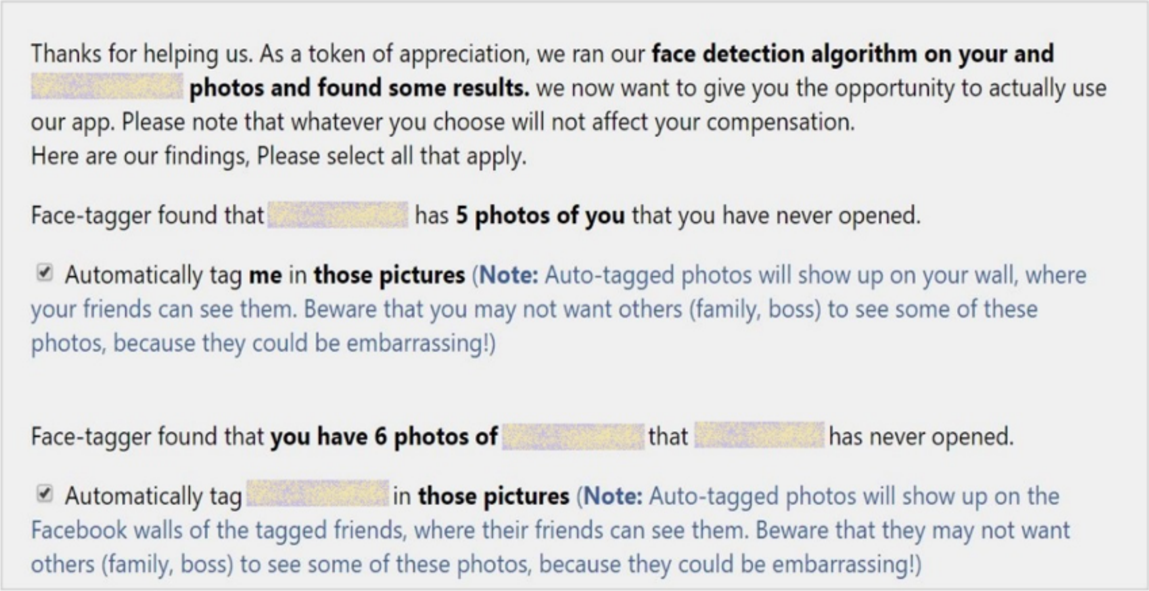
In the pilot study, I provided participants with the opportunity to tag themselves in all their friends' photos and to tag their all their friends in all their own photos. However, no one (out of 50) chose to tag themselves or their friends regardless of the default, framing, or justification message: arguably, they perceived the risk associated with this tagging feature as too high. While their choice meant that I could not collect useful data, it also demonstrated that they made active, deliberate decisions (i.e., all participants in the tag-by-default conditions purposefully acted to change this setting) and that I used a believable experimental setup (if participants had thought that this app was fake, they would have likely been less careful in their decision practices).

To reduce the overall risk of the scenario in the main study, I subsequently reduced the scope of the auto-tagging procedure. Specifically, I added a question in the pre-questionnaire that asked participants to enter the names of three Facebook friends that they regularly interact with. The "decision" phase would then involve a separate page for each friend, which would state that I had "identified" various previously unseen photos that featured the participant together with that friend (in reality, I used a random number between five and 15), and offered participants to tag themselves and/or tag their friend in those particular photos (see Figure 3.3). After interviewing five graduate students about this new decision scenario, I concluded that this procedure would decrease the overall risk and increase users' tendency to accept the tagging.

Finally, I debriefed participants about the experiment's purpose and that the auto-tagger had not in fact tagged any of their photos. Figure 3.4 summarizes the experimental setup.

3.2.2.3 Manipulations

I followed a 2 x 2 x 5 between-subjects design, and randomly assigned participants to one of the conditions. Like most existing studies on defaults and framing, I combined a default setting manipulation (accept versus reject) with a framing manipulation (positive versus negative). I show this 2 x 2 design in Table 3.1. I also added a "justification" manipulation with two rationale-based justifications (one with a positive valence and one with a negative valence), two normative justifications (likewise, one positive and one negative), and a condition without any justification. As such, one can see the justification manipulation as an interaction between "justification type"



Thanks for helping us. As a token of appreciation, we ran our **face detection algorithm on your and** [redacted] **photos and found some results.** we now want to give you the opportunity to actually use our app. Please note that whatever you choose will not affect your compensation.
Here are our findings, Please select all that apply.

Face-tagger found that [redacted] has **5 photos of you** that you have never opened.

☑ Automatically tag **me** in **those pictures** (**Note:** Auto-tagged photos will show up on your wall, where your friends can see them. Beware that you may not want others (family, boss) to see some of these photos, because they could be embarrassing!)

Face-tagger found that **you have 6 photos of** [redacted] that [redacted] has never opened.

☑ Automatically tag [redacted] in **those pictures** (**Note:** Auto-tagged photos will show up on the Facebook walls of the tagged friends, where their friends can see them. Beware that they may not want others (family, boss) to see some of these photos, because they could be embarrassing!)

Figure 3.3: An Example Experimental Condition (Accept by Default, Positive Framing, Negative Rationale-based Justification) in the "Decision" Phase

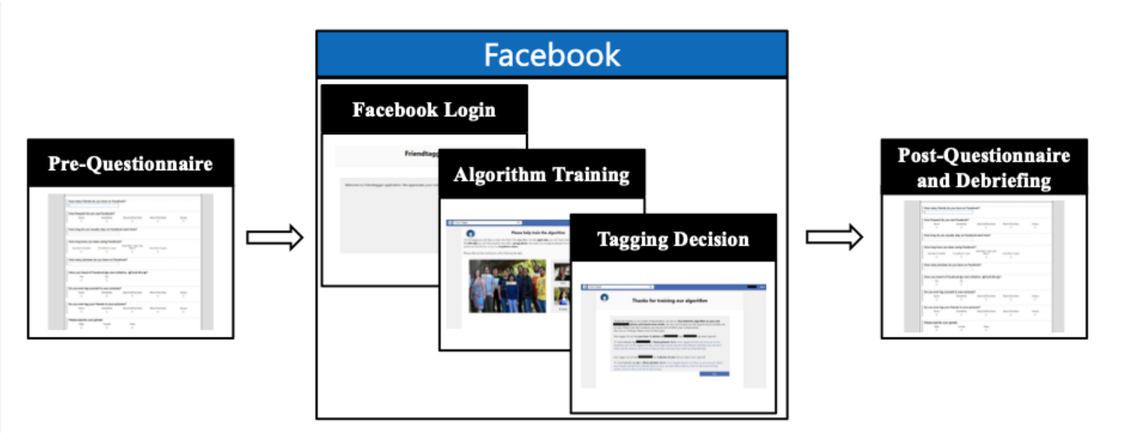


Figure 3.4: An Overview of the Experimental Setup

(none, rationale-based, normative) and "justification valence" (positive, negative) where the "none" baseline condition has no valence.

The descriptive social norm justification indicates that either a small minority (i.e., 3%) or a large majority (i.e., 97%) of all other participants chose to use the automated tagging procedure. To operationalize the rationale-based justification, I conducted a focus group with five graduate students in which I discussed the potential messages to use so that others would infer whether they "ought to" use the application or not. I concluded that talking about tagging's positive aspects

Presentation	Default	Framing
☒ Automatically tag me in those photos.	Accept	Positive
☐ Automatically tag me in those photos.	Reject	Positive
☒ Do NOT automatically tag me in those photos.	Reject	Negative
☐ Do NOT automatically tag me in those photos.	Accept	Negative

Table 3.1: The framing and default conditions

(”tagging may increase your social bond”) would elicit a positive rationale, while talking about negative aspects (”the tagged photos could be embarrassing”) would elicit a negative rationale. Figure 3.3 shows an example scenario with a positive framing, a positive default, and a positive rationale-based justification. In total, I used the following manipulations:

Default (see Table 3.1):

1. Accept (tag) by default
2. Reject (do not tag) by default

Framing (see Table 3.1):

1. Positive (”automatically tag my friends in my photos”)
2. Negative (”do NOT automatically tag my friends in my photos”)

Justification:

1. Negative descriptive social norm-based (”normative”) justification
   - ”(Note: 3% of our study participants chose to tag themselves or their friends)”
2. Positive normative justification
   - ”(Note: 97% of our study participants chose to tag themselves or their friends)”
3. Negative rationale-based justification
   - ”(Note: auto-tagged photos will show up on the Facebook walls of the tagged friends where their friends can see them. Beware that they may not want others (parents, boss) to see some of these photos, because they could be embarrassing!)”
4. Positive rationale-based justification

- "(Note: auto-tagged photos will show up on the Facebook walls of the tagged friends, where their friends can see them. This will strengthen your friendship and let your friends relive the good times they had with you!)"

5. None

3.2.3 Dependent Variable: Tagging Rate

I recorded the participants' decision to tag or not to tag themselves (or their friends) as the dependent variable. In the analysis, I refer to this variable as the "tagging rate". A higher tagging rate in a positive framing or default condition and a lower tagging rate in a negative framing or default condition indicate more mindless compliance. In these instances, people are more likely to simply follow the apparent cues rather than engaging in elaborate thought.

3.3 Results

On average, the participants were 39 years old and checked their Facebook once a day. They spent more than 30 minutes and less than one hour on Facebook in each session. Each participant in the study made six yes/no decisions: for each of the three listed friends, they indicated whether they allowed the auto-tagger to tag their friend in their photos and whether they allowed it to tag themselves in their friend's photos. I conducted the analysis using a maximum likelihood and weighted least square mean and variance estimator in Mplus V 7.4. I used a generalized linear mixed effects model for the analysis: a multilevel logistic regression with a random intercept to account for repeated measurements per participant. Furthermore, I studied the decision to allow or prevent the auto-tagger (i.e., the tagging rate) as the dependent variable and the default, framing, and different justifications as the independent variables. In my analyses, I considered justification as an interaction between "justification type" (none, rationale based, normative) and "justification valence" (positive, negative) with no distinction in valence in the baseline (no justification) condition.

3.3.0.1 Main Effects of Defaults and Framing

I first analyzed the framing and default effects regardless of other manipulations. Table 3.2 shows the outcome of the analysis with centered framing and default effects. In line with previous work, I found that framing had a significant main effect; the model estimated participants to have

Presentation	Odds ratio	p-value (two-tailed test)
Intercept	0.428	
Default (tag vs. do not tag)	2.436	< 0.001
Framing (pos. vs. neg.)	1.967	< 0.001
Default x framing	1.023	0.929
Note: n = 1084, intercept = overall odds.		

Table 3.2: The main and interaction effects of framing and defaults.

1.967 times higher odds to allow the auto-tagger to tag the identified photos in the positive framing condition than in the negative framing condition ($p < 0.001$). Thus, H1 was supported.

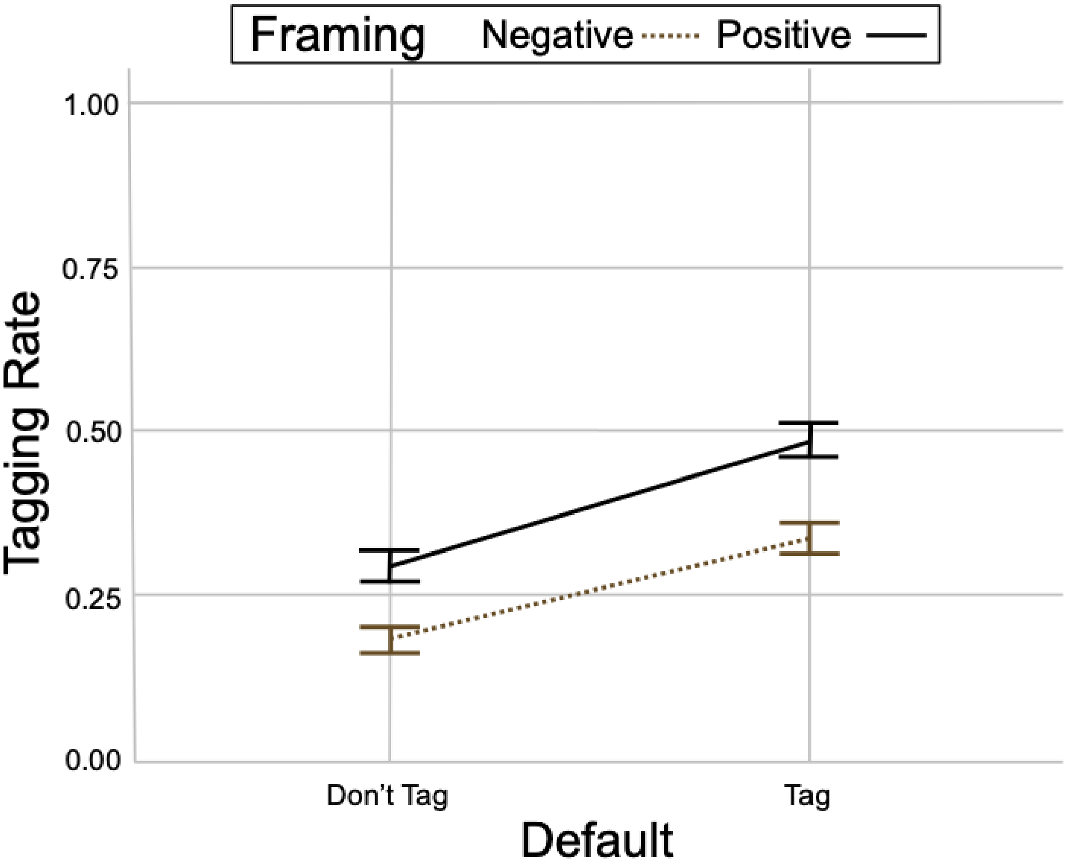


Figure 3.5: The Main Effects of Defaults and Framing on Participants' Tagging Rate

Likewise, I found that defaults had a significant main effect: participants had 2.436 times higher odds to allow the auto-tagger to tag the identified photos in the accept-by-default condition than in the reject-by-default condition ($p < 0.001$). Hence, I also found support for H2.

Finally, in line with previous work, there was no interaction effect between defaults and framing ($p = 0.929$). Figure 3.5 displays the framing and default effects and that their effects were additive (no interaction effect).

3.3.1 Justifications as a Moderator

To investigate H3 and H4, I tested whether normative and/or rationale-based justifications significantly moderated the effect of framing and/or default-induced compliances. To this end, I ran separate factorial models for framing and defaults. I present the results below.

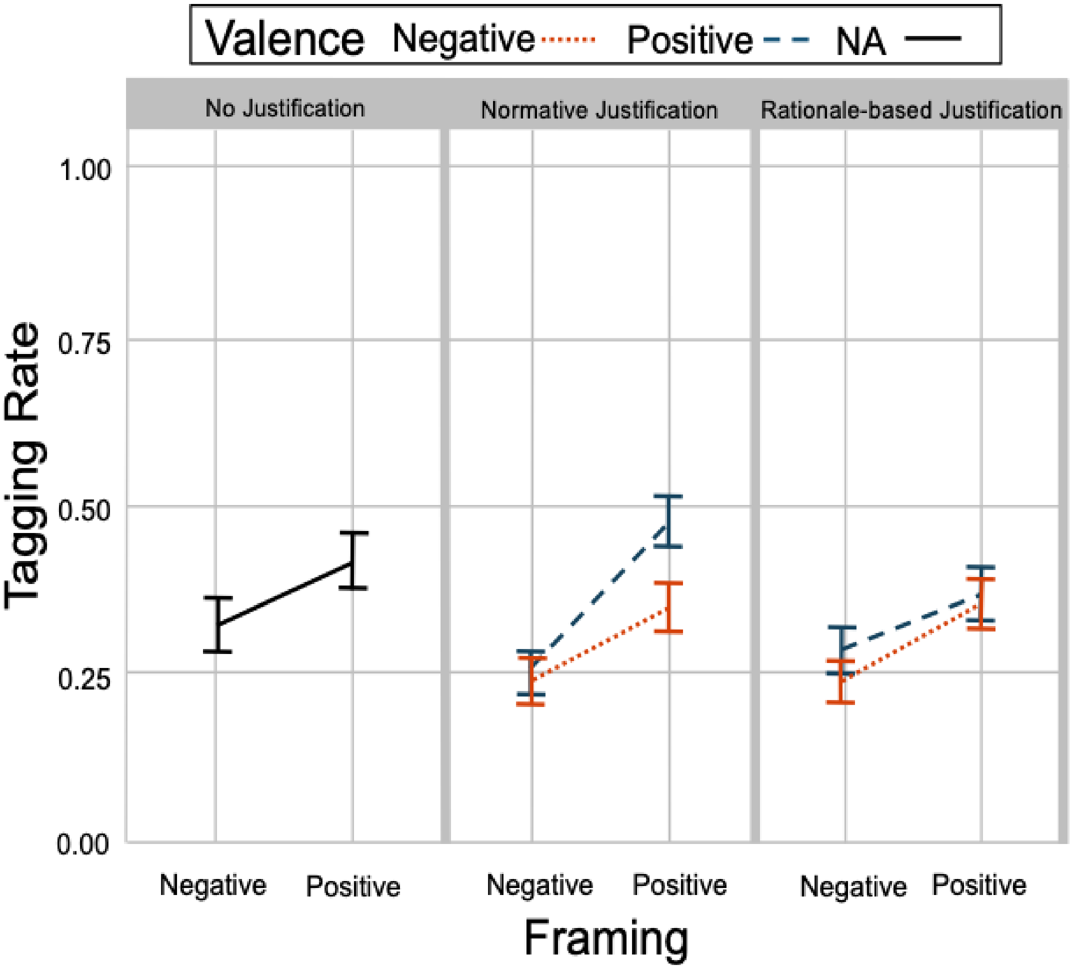


Figure 3.6: A Plot of the Tagging Rates Split by Framing and Justification (Type and Valence)

	Odds ratio	*p*-value
Intercept	0.541	
Justification type (vs. none)		
Normative	0.812	.265
Rationale based	0.747	.128
Justification type x valence		
Normative	1.382	.093
Rationale based	1.180	.429
Framing	1.561	.166
Framing x justification type		
Normative	1.459	.312
Rationale based	1.075	.851
Framing x justification type x valence		
Normative	1.636	.202
Rationale based	0.823	.642

Table 3.3: The Outcomes of of the Multilevel Logistic Regression with Random Intercept Testing the Effect of Framing and Justifications on Participants' Tagging Rate (Note: n = 1084, intercept is overall odds in the no-justification condition; p-value denotes two-tailed significance)

3.3.1.1 Justifications as a Moderator of Framing Effects

I first ran a factorial model with framing, justification type, and valence. I centered framing and justification valence but dummy-coded justification type with "none" as its baseline. Table 3.3 shows the outcome of this analysis, and Figure 3.6 depicts the results. Note that justification valence had no main effect or two-way interaction with framing because the baseline condition (no justification) had no valence. Hence, justification valence only makes sense as an interaction with justification type. I first ruled out any main effects of justifications. Table 3.3 shows that neither the normative justifications ($p = 0.265$) nor the rationale-based justifications ($p = 0.128$) had a main effect on participants' tagging rate. Furthermore, positive and negative normative justifications were not significantly different ($p = 0.093$), nor were positive and negative rationale-based justifications ($p = 0.429$).

I then considered whether the justifications moderated the framing effect. In the "no justification" condition, framing did not have a significant overall effect ($p = 0.166$). I found no significant overall interaction between framing and justification type ($p = 0.312$ and $p = 0.851$) or between framing, justification type, and valence ($p = 0.202$ and $p = 0.642$). Hence, in contrast to H3 and H4, I found normative and rationale-based justifications did not moderate the framing effect.

Notably, when combined with a positively framed request, the results showed that participants had 1.335 times higher odds to allow the auto-tagger to tag the identified photos with

	Odds ratio	*p*-value
Intercept	0.550	
Justification type (vs. none)		
Normative	0.779	.177
Rationale based	0.706	.067
Justification type x valence		
Normative	1.446	.055
Rationale based	1.202	.376
Default (tag vs. do not tag)	1.162	.635
Justification type x default		
Normative	2.119	.043
Rationale based	2.780	.007
Default x justification type x valence		
Normative	0.983	.967
Rationale based	0.789	.571

Table 3.4: The Outcomes of the Multilevel Logistic Regression with Random Intercept Testing the Effect of Defaults and Justifications on Participants' Tagging Rate

the positive normative justification compared to the negative normative justification ($p = 0.027$), whereas the results showed more or less equal odds for the negatively framed request ($p = 0.814$, see Figure 3.6).

3.3.1.2 Justifications as a Moderator of Default Effects

To investigate the effect that justifications and valences had on default-induced compliance, I ran a similar factorial model with defaults, justification type, and valence. Table 3.3 shows the outcome of this analysis, and Figure 3.7 depicts the results.

The results showed that justification type and its interaction with valence had the same main effect as in the previous model, so I do not reiterate the discussion at this point.

In the "no justification" condition, the results suggest that participants had 1.162 times higher odds to allow the auto-tagger to tag the identified photos in the accept-by-default condition than in the reject-by-default condition. However, this effect was not significant ($p = 0.635$). Figure 3.7 suggests that the default effect was stronger alongside a justification. Particularly, compared to the no-justification condition, default had a 2.119 times stronger effect alongside a normative justification ($p = 0.043$) and a 2.780 times stronger effect alongside a rationale-based justification ($p = 0.007$). Interestingly, I found no three-way interaction between defaults, justification type, and valence ($p = 0.967$ and $p = 0.571$), which suggests that justifications had a default-exacerbating effect regardless of their valence. Indeed, Figure 3.7 shows that the default effect was more pronounced

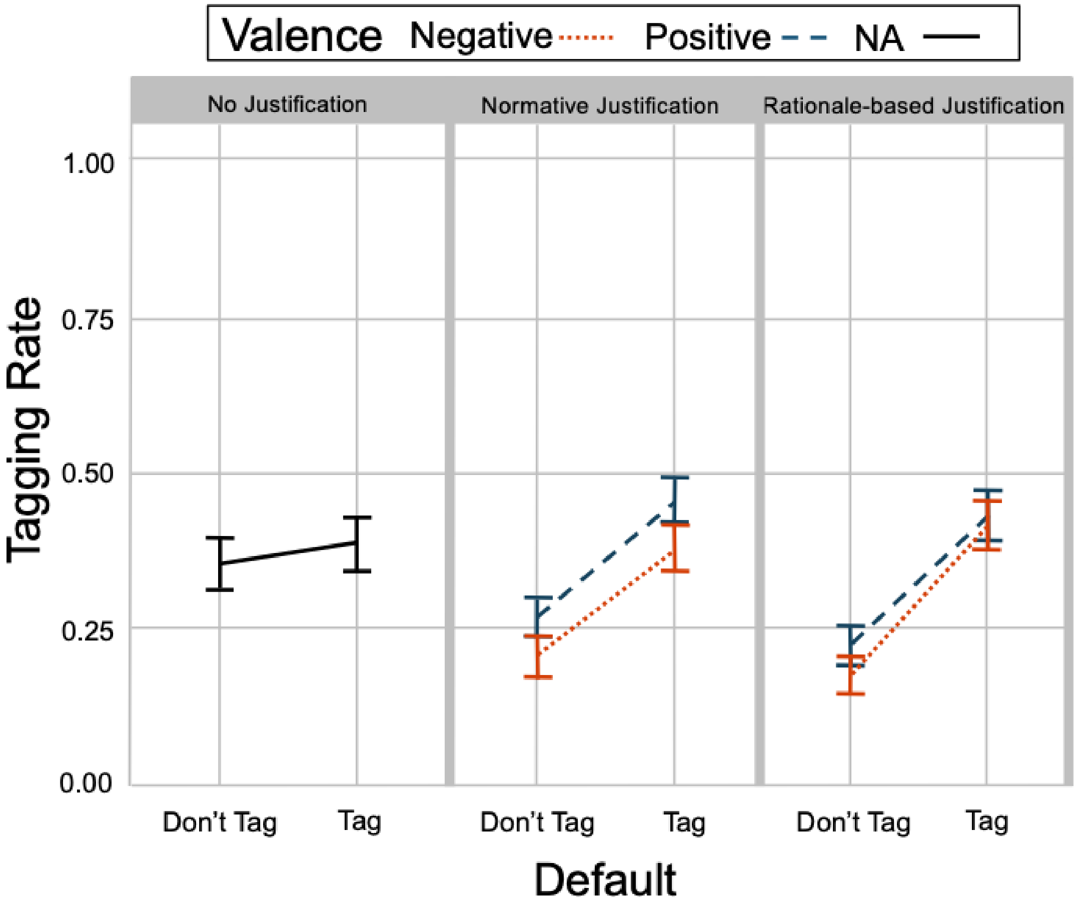


Figure 3.7: A Plot of the Tagging Rates Split by Default and Justification (Type and Valence)

alongside both positive and negative normative and rationale-based justifications. Thus, H3 and H4 were partially supported.

3.4 Discussion

In this chapter, I investigate the moderating effect that justifications have on framing and default induced mindless compliance in the context of privacy decision making. To this end, I developed a realistic scenario in which I introduced normative and rationale-based justifications to different framing and default scenarios. I then tested the moderating effect that these justifications had in a 2 x 2 x 5 between-subjects experimental setting and summarize the results in Figure 3.8.

Regarding the main effects, I replicated the existence of framing (H1) and default (H2) effects

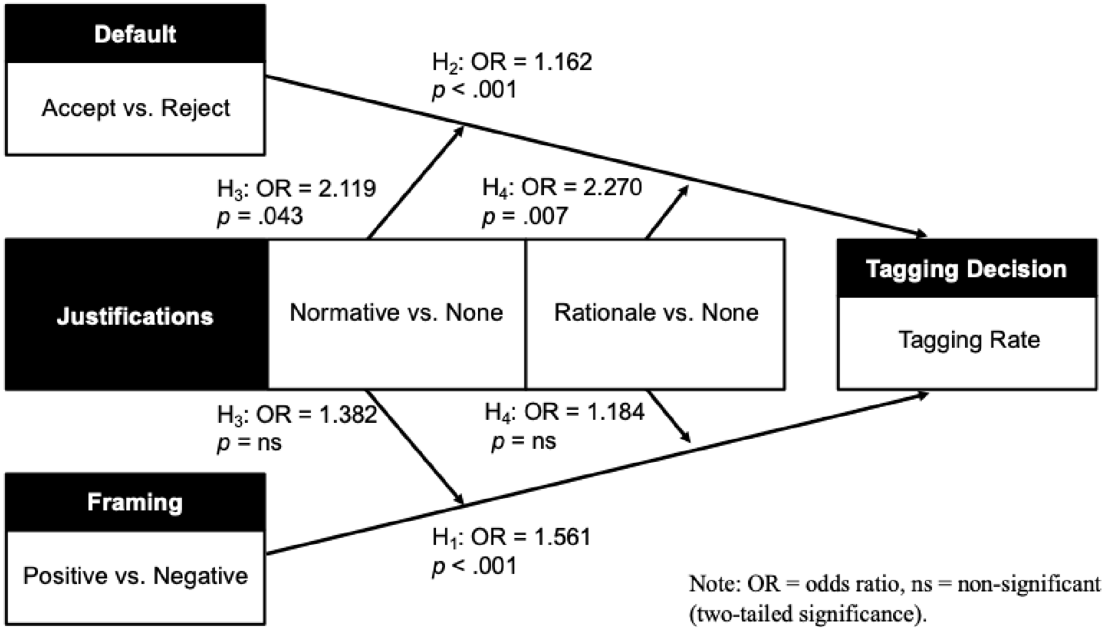


Figure 3.8: Summary of the Findings

in the photo-tagging context on Facebook. Companies commonly leverage these effects to nudge users to comply with their privacy requirements. In line with existing research, I found that positive framing led to higher tagging rates than negative framing. Similarly, I found that accept-by-default settings led to higher tagging rates than reject-by-default settings. In contrast to previous work, I conducted the experiment in a realistic environment. Hence, I confirm corporate assumptions that default and framing effects do not occur only in studies with unmotivated participants: these effects transfer to scenarios with perceivable real-world consequences. Indeed, the remarkable results from the pilot study suggest that participants definitely paid attention.

The prevalence and pervasiveness of framing and default effects in this study suggest that users do not purely determine their preferences a priori but that they construct them (at least to some extent) in a given situation [44]. Since default and framing effects can induce compliance, online applications can use them to strongly and significantly nudge users to choose certain settings. Indeed, Figure 3.5 shows that compliance in this study rose from 19 percent in the negative defaults, negative framing condition to 49 percent in the positive default, positive framing condition.

Regarding the main effects of the newly introduced justification, neither normative justifications nor rationale-based justifications yielded a significant main effect on the tagging decision.

This study examined the moderating effect that normative and rationale-based justifications had on the compliance-inducing framing and defaults (H3 and H4). Normative justifications did not significantly moderate the compliance-inducing effect of framing (p = .325). However, Figure 3.6 shows a notable difference between the positive and negative normative justification for positive framing ($p = 0.027$) but not for negative framing ($p = 0.814$).

Previous work explains the framing effect as an injunctive social norm [213, 271], and Cialdini et al. [80] argue that a sufficiently salient descriptive norm can override such an injunctive norm and, thereby, cause a herding effect [26, 137]. While my results did not show that the descriptive normative justification overrode the injunctive norm of framing, they suggest a herding effect when both the framing and descriptive norm were positive. This finding suggests that participants did not see framing as an injunctive norm but rather as a vantage point from which to consider the descriptive norm. In this case, a herding effect may require congruence between framing and descriptive norm.

The latter argument would suggest that a negative normative justification might also decrease the tagging rates when the framing is negative. However, Figure 3.6 shows that the negative normative justification did not further reduce the tagging rate in the negative framing condition possibly because I presented the normative justification as a lack of support for using the auto-tagger ("3% of others use the system") rather than as support for not using the auto-tagger (i.e., "97% of others do not use the system"). Arguably, the latter could have triggered the herding effect in the negatively framed conditions. Future studies can implement this alternative justification message to test whether the herding effect still occurs when the justification addresses what the majority does.

Whereas neither of the justifications significantly moderated the framing effect, I found that normative and rationale-based justifications moderated the default effect. As Figure 3.7 shows, the justifications increased the likelihood that a user would comply with the default setting. Notably, while valence had a small effect for the normative justification (p =.055), rationale-based justification had an effect regardless of the valence and even when the justification was incongruent with the default setting. This finding concurs with Langer et al.'s finding [182] that, for small favors, people do not process the justification but rather accept it at face value.

This study extends Langer et al.'s [182] work in three ways. First, it shows that their findings extend to an online environment. Second, while Langer et al. compared plausible and placebic justifications, this study found that even justifications that were incongruent with a request increase compliance with it. Third, while Langer et al. [182] did not consider manipulating the default and framing of the request (the request in their study can be considered a positively framed accept-by-default request), this study shows that a rationale-based justification increased the likelihood that participants would comply with the default option whether that be a positive default or a negative default. The fact that the overall effect of rationale-based justifications and the interaction effect between these justifications and valence were not significant (p =.376, p =.571) supports this claim: rationale-based justifications did not have an effect other than to exacerbate the default effect.

Overall, this study shows that rationale-based justifications can indeed moderate the mindless compliance that defaults induce. However, rather than motivating people to think and, thereby, overcome the default effect, rationale-based justifications are instead used as a means to save cognitive effort: people seem not to process these justifications and instead assume that they support the default option. As such, the rationale-based justifications increased rather than decreased default-induced compliance. Similarly, the results suggest that normative justifications exacerbate default-induced compliance as well. The additionally marginally significant effects of the valence of normative justifications indicate that people may process their meaning to some extent but not to the extent that they reduce (let alone overcome) default-induced mindless compliance.

Policy makers who require organizations to seek informed consent for their data-collection practices may find value in this result. The results show that, rather than reducing existing biases, informing users with justifications actually exacerbates their mindless compliance and, thereby, endangers their privacy. Furthermore, companies should be careful when implementing warning messages. If users mistake a warning message for a justification, it could nudge them towards mindless compliance rather than a cautious choice.

3.5 Limitations and Future Work

One must consider the contributions of this study in the light of its limitations, which also provide a basis for future research. First, we cannot generalize these findings beyond Facebook applications and the U.S. population. Bélanger and Crossler [41] criticize information privacy research for heavily depending on U.S.-centric student samples. While this study partly acknowledged this criticism by recruiting from a nationwide, non-student sample, it was restricted to a U.S.-based sample. The universality of default and framing effects suggests that we can generalize the results to other populations, but we need future work to provide conclusive evidence about the results' robustness.

Likewise, considering that privacy decisions depend on the situation [186], we need to acknowledge that, in this study's baseline condition, only approximately 25 percent of participants opted in to using the auto-tagger, and over 50 percent of participants opted out. In combination with the pre-test results (where everybody opted not to use the auto-tagger), this finding suggest that participants were rather skeptical about the app's proposition to begin with. However, the effects occurred despite this fact, and situations with lower privacy stakes would not likely have exacerbated them.

In addition, since I conducted the study on Facebook, some users may have assumed that Facebook moderates apps for safety reasons. Consequently, their trust in the app might correlate with their trust in the platform. Future work should examine if users presume providers to exert moderating control and whether such an effect can influence trust and disclosure.

Furthermore, I suggest future studies to consider additional variables. To test for justifications' general efficacy, future research must include a neutral default and framing condition (e.g., by asking users to write ”yes” or ”no” if they want to participate or not) to ultimately assess justifications' main effects. In a similar vein, future work can also consider the opposite normative justifications (xx% of others do not use the system) to test if it would cause a herding effect toward the negatively framed option.

Finally, this study was conducted in a static environment. To analyze whether framing and default effects dissipate over time, future research could apply a longitudinal approach with repeated decisions.

3.6 Conclusion

According to Venturini and Rogers [308], the Cambridge Analytica scandal had at least one merit: it generated significant discussion around people's expectations about how organizations use social media data. The scandal also pushed Facebook's executives to explore how they can prevent parties from misusing data that social media platforms collect [308]. Although Facebook claims that it collects data based on users' own choices, individuals who used the app in the Cambridge Analytica case essentially gave mindless consent by default [266] rather than by actively opting in to its data-collection practices.

Users care about protecting their individual privacy [323]. Framing and default biases threaten individuals' privacy by subconsciously nudging them to comply with disclosure requests and, thus, disclose private information they may not actually want to share. To test the effect that justifications had on framing- and default-induced compliance, I set up an experiment that offered users the ability to give up some collective privacy (identifying oneself or friends in a photo) in return for gratification (creating a shared social experience around these photos). The justifications did not affect the framing-induced mindless compliances and, far from reducing default-induced mindless compliance, the rationale-based justifications further increased the default effects.

These findings provide considerable contributions to human decision-making research and the research on defaults, framing, and justifications in particular. Importantly, this work demonstrates that framing and default effects persist in realistic decision scenarios. Moreover, the decision scenario in this study moves work on defaults and framing to the essential domain of social privacy and particularly to collective privacy management [143]. Tagging oneself in one's friends' photos includes those photos on one's timeline, makes them more easily accessible to one's friends, and establishes a relationship between oneself and the friends who posted the photos. Likewise, tagging one's friends in one's own photos will associate oneself with that friend and make oneself accessible to all friends of the tagged friends. The interdependent nature of privacy management regarding tagged photos means that both users' personal preferences and the social norms that they perceive the individuals whom their decisions affect to have (i.e., their friends) likely influence their privacy decisions about tagging.

Likewise, this work expands on previous work about various types of justifications. Regarding rationale-based justifications, this research expand Langer et al.'s [182] work on "mindless compliance" by demonstrating that even a rationale-based justification that is incongruent with a request can induce compliance with it arguably because people forego processing the justification and instead simply assume that any justification will support the default. In addition, Langer et al.'s [182] findings do not only hold up for a positive default but also apply to a negative default.

Regarding normative justifications, this work showed that the anticipated herding effect [26] only in the positive framing condition, which suggests that herding requires a congruent framing to be effective. However, this effect was only marginally statistically significant and cannot confirm Cialdini et al.'s [80] general theory that a sufficiently salient descriptive social norm overrides an injunctive social norm.

These findings point towards the dangers of using justifications in combination with established biases that may induce users to make heuristic decisions. The results show that justifications do not eliminate these heuristic influences but may, at times, even exacerbate them. Policy makers must carefully consider these findings when requiring platform managers to justify their data-collection practices lest they accidentally urge users to disclose their personal information against their will. Also, the results serve to warn users to mind these effects when making privacy decisions.

Furthermore, Bélanger and Crossler [41] call for more IS research on design and action. Hirschheim [132] discusses the need for theoretical work to develop practical solutions that directly pertain to problems in industry. This experiment was a design and action study in which I designed an environment and empowered users when making a privacy decision by introducing interventions to reduce mindless compliance. The fact that the interventions had an opposite effect evidences that such design and action research serves an extremely important role for society. This work also closely ties to industry since it was conducted on Facebook, the world's most popular social media platform, and examined a significant issue it and many other organizations face (i.e., privacy).

Overall, this chapter showcases that privacy decisions are not necessarily a byproduct of a rational process. This chapter showed that framing and default manipulations could induce compliance. Participants' lack of attention to the justification messages further supports this finding, that this compliance is not a result of effort expenditure. While negative justifications should rationally reduce disclosure, they indeed exacerbated the default effect. Researchers need to adopt a heuristic framework even when operationalizing cognitive manipulations, as users' decisions may be partially "mindless".

Chapter 4

Older Adults Care About Their Privacy

While past research has highlighted age-related differences in privacy awareness, concerns, and protective behaviors, none of these studies have examined differences in the *privacy decision-making processes* of older and younger adults. Understanding how age is related to decision-making processes, rather than privacy attitudes and outcomes, can help us better understand the choices younger and older adults make regarding their privacy and the factors that must be considered when designing technologies to assist with their privacy decision-making. The study presented in this chapter is one of the first empirical attempts to investigate differences in the *mechanisms* by which older and younger adults make privacy decisions—the decision process that leads them to either disclose their data or withhold it from disclosure. As such, this chapter contributes to the literature by studying age differences in the privacy decision-making *process* rather than merely focusing on the decision *outcomes*. To this end, I address the following high-level research questions:

RQ1: *Do older adults disclose more personal information online than younger adults?*

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

To answer these research questions, I adopt a dual-route privacy framework. In chapter 2, I discussed the importance of integrating rational and heuristic frameworks. In this chapter, I present a study in which I designed an experiment with respect to two opposing privacy decision-making frameworks (i.e., privacy calculus [161, 93, 176, 94] and heuristic decision-making [6, 313]). I integrated these two frameworks into a cohesive theoretical model to understand how these constructs influenced older and younger adults' disclosure decisions.

To that, I recruited 94 participants to take part in a web-based user study. The recruitment criteria was based on two different age groups—younger adults (ages 18-22) and older adults (65+)—to compare differences between these two groups. First, I presented a fictitious financial planning app (i.e., "CreditPush") to the participants. I described CreditPush as a financial app, which generates recommendations to help users improve their credit score and financial situation. Second, I asked participants to disclose various types of personal information (e.g., bank account balances, annual income, credit score) to use the app. I then asked participants to self-report on privacy-related constructs, including perceived app trust, sensitivity of the data, and benefits of disclosure. I then did a more in-depth analysis on this model based on age group to understand differences between younger adults and older adults in terms of their unique decision-making processes. To test the model, I conducted path analyses to examine the direct effects of the model constructs on the decision to disclose personal information to the app, as well as the moderating effects of age on this decision-making process.

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

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

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

4.1 Theoretical Framework

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

4.1.1 Dependent Variable: Information Disclosure

Information disclosure is a commonly studied outcome variable within privacy research [332, 204, 94, 333, 17, 226] as users' privacy decisions typically involve choosing to withhold or disclose one or more types of personal information. Examples of information disclosure behaviors studied in past privacy research have ranged from whether to share one's financial information to complete an e-commerce transaction [93, 94], one's health data to benefit from a health-app [136] or online health communities [337], one's location to leverage location-based services [332], or one's personal information to use social networking sites [176].

Disclosing personal information may be advantageous for users, as it gives them access to better or more personalized services that leverage this data [332]. For example, while users might be able to browse an e-map in private mode, they must disclose their location to be able to use GPS features. Likewise, in a messaging app users can manually enter the recipient's email or phone number, but giving the app access to the user's contacts enables them to select an existing entry, thereby avoiding the hassle of having to type it themselves. The rewards of disclosure, however, come at the cost of diminished privacy: users may worry that their safety could be compromised if their location data is hacked, or they might fear that the messaging app might use their contact list for promotional activities. Users thus have to decide whether to disclose their information and obtain some gratification or to withhold from disclosure and maintain their privacy. In this study, I treat the decision to disclosure personal information to a fictitious financial planning app as the outcome variable of interest.

4.1.2 Privacy Calculus: Perceived Benefits vs. Costs of Disclosure

As outlined in chapter 2, privacy calculus is a well-studied framework for studying the trade-off between the benefits and costs of the disclosure [185]. However, studies have used different approaches to operationalize these antecedents. In this study, I examined the benefits of disclosure by first asking participants to disclose or withhold several pieces of information to a fictitious financial app. Each of these disclosure decisions involves a trade-off between the rewards and the costs of disclosure. To assess the benefits of disclosure, I asked participants to rate how much they felt the information requested would improve the *quality of recommendations* provided by the app. There is a large body of literature exploring the trade-offs between privacy and personalization [331]. In this study, the quality of the recommendation served as a form of personalization [332], thus a potential benefit of disclosure when using a financial planning app.

To assess costs associated with disclosure, I measured *perceived data sensitivity.* Perceived data sensitivity has been associated with heightened disclosure risks [193], privacy concerns [329], and fewer information disclosures [204] in previous literature. Based on the privacy calculus framework and the aforementioned operationalizations of costs and benefits, I pose the following hypotheses:

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

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

4.1.3 App Trust as a Heuristic for Disclosure

A heuristic is a strategic or mental shortcut that often involves considering some information and discarding others when making a decision [141]. Some scholars study trust as a heuristic [339, 189, 322]. Lewicki et al. [189], for example, present trust as an “affect heuristic” that shapes judgements especially for some decision makers who rely on this heuristic and ignore other information when making a decision. Therefore, a heuristic view of trust suggests that high trust may streamline the disclosure decision making process [265]. While most studies in the field do not conceptualize trust as a heuristic, trust has been commonly used as an antecedent in studies that use the privacy calculus framework [67, 84]. Xu et al. [332], for example, showed that users who have more trust in a service provider also have lower perceived levels of privacy risks and are more willing to disclose information to that service provider. Gong et al. [118] studied people’s attitudes towards online health services. They not only showed that users with high trust have lower risk perceptions, but they also found that highly trusting users perceive higher levels of benefit. I use a 4-item construct to measure a user's trust in the app adopted from previous literature [142, 217, 166]. In line with past findings, I pose the following hypotheses:

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

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

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

4.1.4 Older Adults vs. Younger Adults and Disclosure

A person's age may have two distinctive effects on privacy decisions: it can be associated with higher or lower levels of disclosure (i.e., a main effect on disclosure), or it can influence the *process* by which information disclosure will come about (i.e., a moderation of the effects in the privacy calculus framework). The former effect has been investigated in considerable detail with privacy literature. In terms of the main effect of age on disclosure, the existing evidence is mixed. Jourard [153] did not find any significant overall relationships between age and self-disclosure. Little et al. [197], on the other hand, found an overall U-shaped trend in disclosure levels in which younger (under 35) and older (above 56) individuals disclose the same amounts of information while individuals from 35 to 55 disclose less information compared to younger and older groups. Meanwhile, other studies have shown that older adults take fewer privacy protective actions, which lead to more online information disclosures [272]. Given these mixed findings, I chose to hypothesize that older adults disclose more personal information online, which makes them more vulnerable to privacy threats. While I do not subscribe to this deficit-based narrative, it is an uncommon practice to test a null hypothesis of no differences, and the primary intention is to investigate whether this deficit-based assumption about older adults holds true. Therefore, H6 corresponds to the RQ1:

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

Meanwhile, understanding the effect of age on the process by which information disclosure occurs is a novel contribution of this work. While there are several studies in the information privacy literature highlighting privacy deficits around how older adults manage their digital privacy, these studies often build on the premise that older adults are not as technologically skilled or as privacy-aware as their younger counterparts, and therefore, are more prone to privacy threats. These studies focus on the relative *value* of the antecedents of disclosure (e.g., whether older adults have lower privacy awareness [272]), while this chapter explicitly studies differences in the *impact* of these antecedents on participants' privacy decisions (e.g., whether privacy awareness has a different impact on decisions for older than younger adults)—the existence of such differences would indicate that older adults' decision mechanisms are different from those of younger adults. This work is one of the first to examine the moderating effects of age on the privacy calculus and heuristic decision-making processes of younger versus older adults.

Figure 4.1 summarizes the hypothesized relationships between users' perceptions of app trust, sensitivity of the data, quality of the recommendation, and disclosure in the model (H1-H5; see Sections 4.1–4.1.3). I also test the assumption that older adults disclose more information online than younger adults (H6/RQ1). However, a key contribution of this work is that I go beyond these direct effects and examine the moderating effects of age group (i.e., older vs. younger adults) on the privacy decision-making processes associated with the model constructs (RQ2). Due to the novel and exploratory nature of this analysis, I chose not to explicitly pose hypotheses for the moderating effects of age group; rather, I report the relationships that were found in the results.

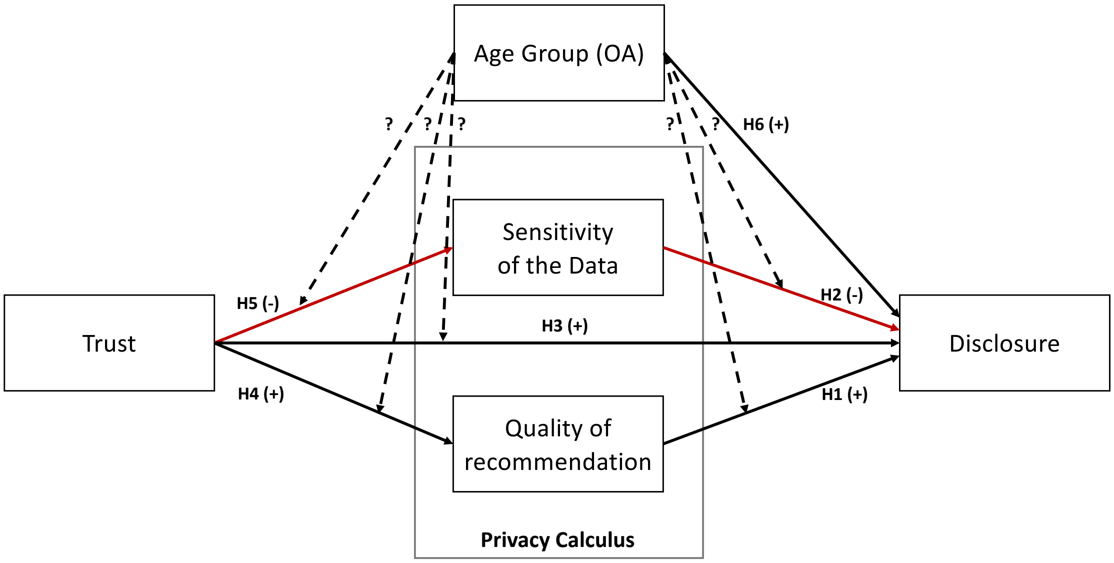
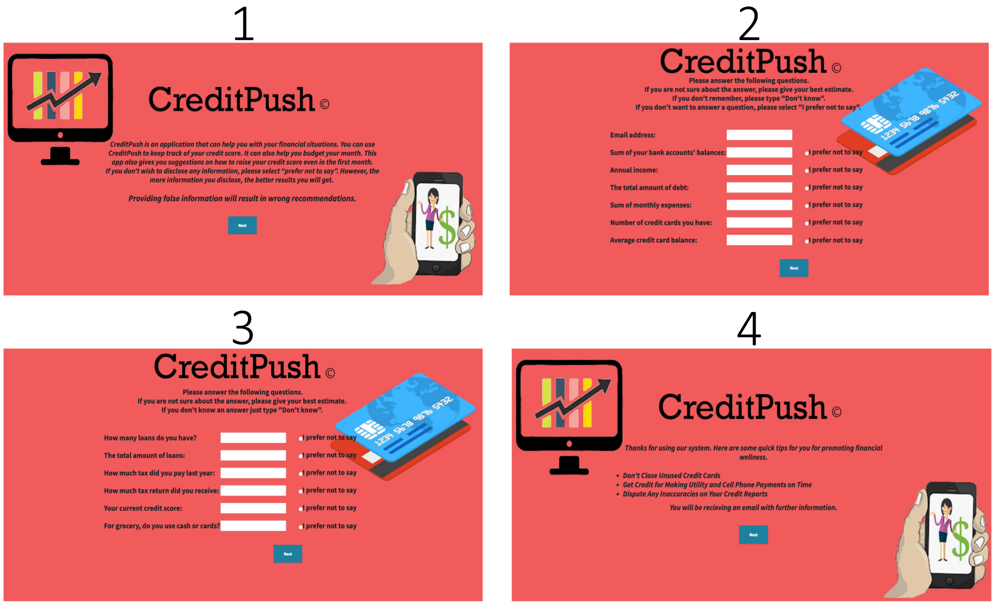


Figure 4.1: The hypothesized model and research questions

4.2 Methods

4.2.1 Study Overview

To address the research questions and test the hypothesized model, I designed an online study. One of the objectives in this study was to overcome the shortcomings of studies with hypothetical scenarios and obtain ecological validity. Therefore, I developed a realistic yet fictitious web application called CreditPush: a financial app which purportedly could provide its users with tips to increase their credit score. After reading the consent form and agreeing to participate in the study, participants were redirected to the app. The first page of the app had some general information about its purpose. In the second and the third page, participants were asked several personal data-items (See Table 4.1 for a list of data-items) and could choose to disclose or not to disclose their data. Figure 4.2 presents some screenshots from the app. After interacting with the app, participants were redirected to a survey where I measured the constructs described in the research framework (see Figure 4.3).



CreditPush ©

CreditPush is an application that can help you with your financial situations. You can use CreditPush to keep track of your credit score. It can also help you budget your month. This app also gives you suggestions on how to raise your credit score even in the first month. If you don't wish to disclose any information, please select "prefer not to say". However, the more information you disclose, the better results you will get.

Providing false information will result in wrong recommendations.

CreditPush ©

Please answer the following questions.
If you are not sure about the answer, please give your best estimate.
If you don't remember, please type "Don't know".
If you don't want to answer a question, please select "I prefer not to say".

Email address:
Sum of your bank accounts' balances: ○ I prefer not to say
Annual income: ○ I prefer not to say
The total amount of debt: ○ I prefer not to say
Sum of monthly expenses: ○ I prefer not to say
Number of credit cards you have: ○ I prefer not to say
Average credit card balance: ○ I prefer not to say

CreditPush ©

Please answer the following questions.
If you are not sure about the answer, please give your best estimate.
If you don't know an answer just type "Don't know".

How many loans do you have? ○ I prefer not to say
The total amount of loans: ○ I prefer not to say
How much tax did you pay last year: ○ I prefer not to say
How much tax return did you receive: ○ I prefer not to say
Your current credit score: ○ I prefer not to say
For grocery, do you use cash or cards? ○ I prefer not to say

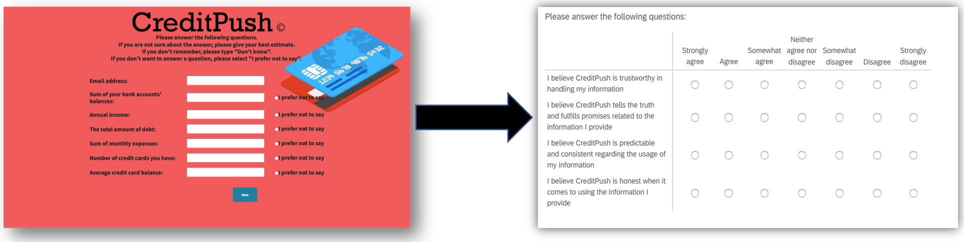
CreditPush ©

Thanks for using our system. Here are some quick tips for you for promoting financial wellness.

- *Don't Close Unused Credit Cards*
- *Get Credit for Making Utility and Cell Phone Payments on Time*
- *Dispute Any Inaccuracies on Your Credit Reports*

You will be recieving an email with further information.

Figure 4.2: Screenshots of the app. In the first page users gain some information about the app, in the second and third pages they disclose (or withhold) information, and in the last page they receive some feedback and then proceed to the surveys.



CreditPush ©

Please answer the following questions.
If you are not sure about the answer, please give your best estimate.
If you don't remember, please type "Don't know".
If you don't want to answer a question, please select "I prefer not to say".

Email address:		
Sum of your bank accounts' balances:		○ I prefer not to say
Annual income:		○ I prefer not to say
The total amount of debt:		○ I prefer not to say
Sum of monthly expenses:		○ I prefer not to say
Number of credit cards you have:		○ I prefer not to say
Average credit card balance:		○ I prefer not to say

Interaction with the app

Please answer the following questions:

	Strongly agree	Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Disagree	Strongly disagree
I believe CreditPush is trustworthy in handling my information	○	○	○	○	○	○	○
I believe CreditPush tells the truth and fulfills promises related to the information I provide	○	○	○	○	○	○	○
I believe CreditPush is predictable and consistent regarding the usage of my information	○	○	○	○	○	○	○
I believe CreditPush is honest when it comes to using the information I provide	○	○	○	○	○	○	○

Questions about sensitivity, relevance, and trust

Figure 4.3: The experimental setup. After interacting with the app, participants were directed to a survey.

4.2.2 Operationalization of Constructs

4.2.2.1 Dependent Variable: Information Disclosure

Participants were given the opportunity to disclose 12 personal information items to the app (see Table 4.1 for a full list of these items). Each of these 12 items were relevant to the context of the app and were chosen after a discussion session with several graduate students. Participants were told that disclosure was not required, but disclosing any of this information could increase the recommendation quality offered by the app. Participants were also instructed that if they were unsure of the exact value of a questionnaire item and they wanted to disclose it, then they could give their best estimates. Prior to the experiment, I had made it clear that participants' incentives were not contingent upon their responses. In addition, participants did not have an incentive to provide false or misleading information, because such information could adversely influence the app-generated recommendations and make the recommendations misleading or inaccurate. In cases that participants were not willing to disclose their data, they could select a ”prefer not to disclose” option. However, to make sure participants did not consider themselves anonymous, disclosing their email address to the app was mandatory. Non-anonymity was important because there are minimal risks associated with disclosing non-identifiable data while being anonymous. I used participants' decision to disclose (or withhold) as the dependent variable. Unlike the majority of past studies, which measure overall *intention to disclose* data with multiple-scale items, I measured actual disclosure decisions of the data items as binary variables (coded as 1 for disclosure and 0 for non-disclosure).

Table 4.1: Descriptive statistics on data-items. Participants were able to disclose or withhold their data. The overall disclosure percentages are reported in this table. Participants were also asked to rate the sensitivity level of each data-item, and specify the extent to which they believe disclosing each data-item would improve the app-generated recommendation quality.

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

4.2.2.2 Independent Variables

Participants were informed that their data would be used to improve app-generated personalized financial advice, and subsequently I measured the extent to which participants believe disclosing each of the items could improve the app-generated recommendations on a 1 (Strongly Disagree) to 7 (Strongly Agree) Likert scale [170]. I also used participants' subjective perceptions of data sensitivity as a proxy for costs of disclosure. Participants were asked about the perceived sensitivity levels of each of the 12 data items on a 4-point Likert scale (Not at all sensitive to very sensitive) [204]. Similar to how I measured disclosure, I also measured the perceived benefits (i.e., quality of recommendation) and costs (i.e., data sensitivity) associated with disclosing each data item individually.

App trust was another independent variable of the study; since trust is an attribute of the app rather than individual data items, measuring it on an item-basis is not applicable. I therefore measured trust of the app using a 4-item construct (e.g. "I believe CreditPush is honest when it comes to using the information I provide"–see Table 4.2 to check other items) which was validated in several previous works [142, 217, 166]. Figure 4.3 shows the experimental setup.

Table 4.2: Trust Items Adopted from Jarvenpaa et al. [142] and Metzger et al. [217]

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

4.2.3 Participant Recruitment

The study sample consisted of older and younger adults. The U.S. Census Bureau and Centers for Disease Control (CDC) define older adults as individuals with the age equal to or above 65 years old and younger adults as individuals aging between 18 and 34 years old [165, 57]. Following these guidelines, I recruited participants within that age range. I initially recruited 117 participants; however, twenty-three participants failed to correctly answer the attention check questions and were excluded from the analysis. Therefore, the sample consisted of 94 participants, including 34 older adults (ages 65 - 86, M=73.59 years, SD=4.28 years), and 60 younger adults (ages 18 - 22, M=19.22 years, SD=1.15 years; see Table 4.3). The younger adults were recruited through a university recruitment system and received extra credit for their participation. The older adults were recruited through email communication and fliers at local community centers, educational locations (i.e., local Osher Lifelong Learning Institutes, college campuses), and retirement communities throughout the Greenville-Anderson-Mauldin, SC metropolitan area. Older adults received a $30 gift card for participating.

The older adults sample also passed the Montreal Cognitive Assessment (MoCA) test which is used for accurately screening mild cognitive impairment, dementia, and normal aging [183, 108]. Research shows that the MoCA test is superior in overall sensitivity for detecting these different cognitive states than other similar tests such as Mini Mental State Exam (MMSE) [254]. Consequently, none of the older adult participants were diagnosed with a neurological illness, such as Alzheimer's disease or stroke. Furthermore, all of the older and younger adult participants had used computer and internet before and therefore were familiar with such technologies. This is important since older adults represent a more heterogeneous population compared to younger adults because their educations, experiences, and health and living conditions are more variable [121, 196]. Lastly, this study was reviewed by an institutional review board and informed consent was obtained from all the participants prior to their participation. Participants were debriefed about the purpose of

Table 4.3: The sample characteristics.

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

the study after their participation.

4.2.4 Data Analysis Approach

During the study, participants made 12 disclosure decisions of financial information relevant to improving the quality of the CreditPush app recommendations. I considered this behavior (whether to disclose or to withhold) as a binary dependent variable. Two of the independent variables were the elements of privacy calculus: participant's subjective perceived sensitivity of each data and their perceived improvement of recommendation quality by disclosing that data. These two variables were repeatedly measured based on the 12 data points of disclosure asked by the app. I also measured the extent participants trust the app with a 4-item pre-validated construct. I used Cronbach's Alpha to re-confirm trust's internal consistency. Cronbach's Alpha being above 0.7 (α = 0.973) suggests a good internal consistency for the trust construct [82]. Therefore, I calculated its sum-score and used it in the model. I standardized trust, perceived sensitivity, and perceived recommendation improvement variables for analysis. I also centered age group variable where OAs with the age of 65 and above were dummy coded as 0.5 and YAs were dummy coded as -0.5. To analyze the data, I conducted a multilevel logistic regression model with a random intercept to account for repeated measurements per participant. I first ran a saturated model [190], which included all paths for two and three-way interaction effects. Then, I trimmed paths that were not significant. Lastly, among the participants, there were 72 females and 22 male participants. Since the sample was not gender-balanced I controlled for participants' gender.

4.3 Results

The model's fit indices suggest a good fit. Although the chi-square test shows a significant misfit of $\chi^2(12) = 24.696, p = 0.016$, having a significant chi-square value is not unexpected in analyses with a relatively large number of records. Scholars used other metrics such as dividing the chi-square value by the degrees of freedom [295, 165]. That value is below 3, which is an indication of a good fit (2.058 in this case). Furthermore, the RMSEA of the model has a 90% confidence interval length of 0.035 and is below the cutoff threshold of 0.05 (RMSEA = 0.031) which is another indicator of a good fit [71].

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

I hypothesized that the perceived improvement of the quality of the recommendations (i.e., disclosure benefits) would be positively associated with participants' information disclosure decisions (H1). However, this hypothesis was not supported. With each one standard deviation increase in perceived benefits, participants were a mere 2.1% more likely to disclose the information, which was not statistically significant ($p = .791$). Yet, there was a significant interaction effect of age group, which is reported in section 4.3.3.

For H2, I found a significant, negative effect of data sensitivity on disclosure. With each one standard deviation increase in data sensitivity, participants were 27.1% less likely to disclose their information to the app ($p < .0001$). Thus, H2 was supported.

4.3.2 The Main Effects of App Trust

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

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

4.3.3 The Effects of Age Group

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

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

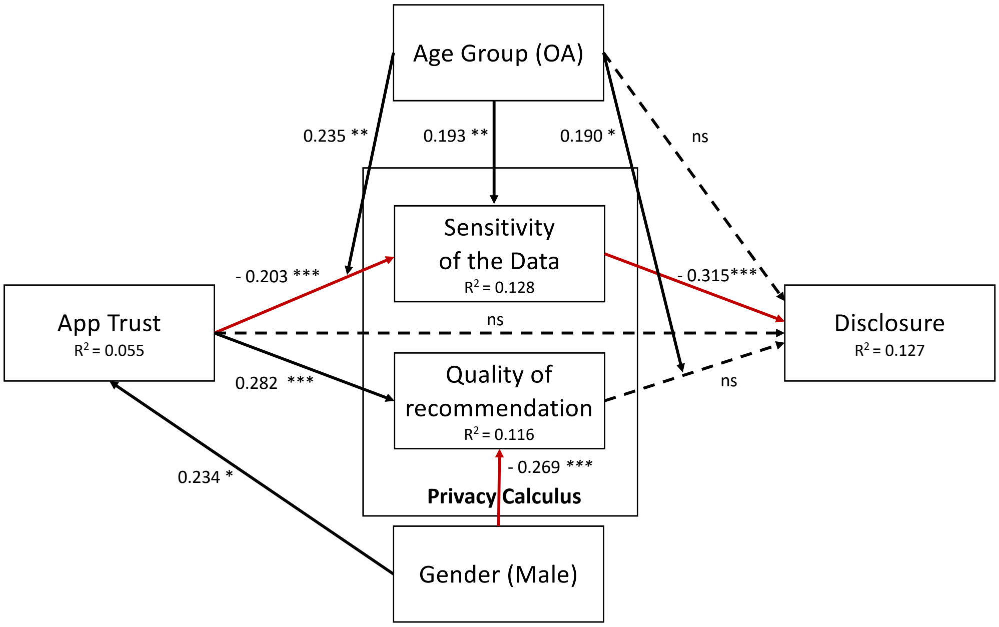
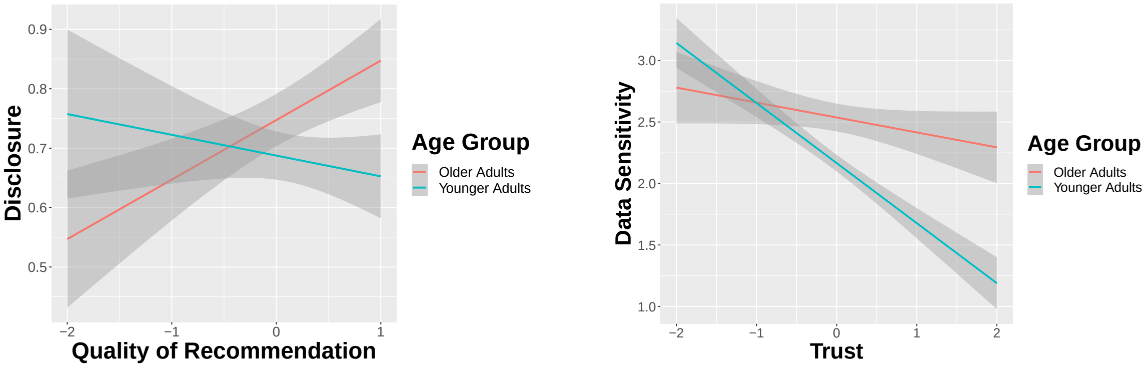


Figure 4.4: The path model including all of the significant findings (ns: not significant, * $p < .05$, ** $p < .01$, *** $p < .001$)
Model

I also found two significant moderating effects of age group. First, age group moderated the relationship between perceived improvement of the quality of the recommendations (i.e., disclosure benefits) and disclosure. Figure 4.5a graphs this effect. For older adults, there was a positive correlation between the perceived improvement to the quality of the recommendations, while for younger adults, this relationship trended in the opposite direction. With each one standard deviation increase in perceived disclosure benefits, older adults were 20.9% more likely to disclose their data



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

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

Figure 4.5: Age group moderates the effect of benefits of disclosure on disclosure (a) and trust on perceived data sensitivity (b).

($p=.031$) compared to younger adults.

In addition, I found that age group moderates the effect of trust on perceived data sensitivity ($p=.001$). Since the main effects of age group and trust on data sensitivity are also significant, all these effects should be studied together. Figure 4.5b shows that while older adults data sensitivity is not a function of trust, younger adults heavily rely on trust such that if they trust the app more they perceive their data being less sensitive.

The negative effect of data sensitivity on disclosure was stronger for older adults than younger adults; with each one standard deviation increase in perceived data sensitivity, older adults were 9% less likely to disclose their data than younger adults. However, this effect did not reach significance ($p = .219$). Lastly, the effect of trust on perceived improvement in recommendation quality and on disclosure were also not significantly moderated by the age group ($p=.350$, $p=.708$).

Figure 5.3 shows the significant direct and moderating effects of age group. All paths not drawn in this model were non-significant. The only non-significant paths (shown with dashed lines) drawn in this model are relationships that were hypothesized in the research framework. Statistically significant negative associations are drawn in red. Table 4.4 summarizes the findings.

Table 4.4: A summary of the findings. Odds Ratios (OR) are calculated for the disclosure decisions where the outcome variable is binomial

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

4.3.4 The Effects of Gender

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

4.4 Discussion

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

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

Privacy calculus assumes that people make calculated decisions [185, 83]. Contrary to this traditional view, research on privacy decision making suggests that decisions are also driven by heuristics [7]. Therefore, scholars developed frameworks to square the privacy calculus and heuristic viewpoints and found that both these viewpoints can work together and complement each other in terms of understanding users' privacy decisions [311]. Likewise, the results show that both viewpoints are accurate when considered together. It follows that focusing on an exclusive rational or heuristic view cannot fully explain the underlying mechanism of privacy decision making.

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

4.4.2 The Privacy Calculus of Older Adults

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

This finding is in line with the psychological literature that suggests that older adults are more likely to think about long-term outcomes and be goal driven compared to younger adults [327, 88, 220]. Worthy et al. [327] suggests that older adults have a model-based way of thinking and are more goal-driven than younger adults. In a model-based system, individuals create a cognitive model of the environment. They are concerned with the way different states of the world are connected to each other [88, 98], think about long-term outcomes [88], and are goal-driven [220]. Gläscher et al.[116] compare the model-based system with the game of chess in which the player seeks future states (or moves) and evaluates the *rewards* associated with them. Although model-based decision making is more computational demanding and effortful, it is also more flexible and can be easier adjusted to the environment [102]. On the other hand, in a model-free system subjects do not simulate a cognitive model of the environment; past experiences and outcomes in one's environment are relied upon less, and heuristics are more likely to govern decisions. Therefore, predictions of future reward outcomes are less pronounced. This model-free way of thinking seemed to be more characteristic of younger adults, which I will discuss next.

4.4.3 The Heuristic of Trust for Younger Adults

The two significant moderating effects of age group shown in Figure 4.5a and 4.5b paint an interesting picture for younger adults. First, younger adults did not seem to weigh the perceived benefits of disclosure (i.e., improved quality of recommendations) in their decision to disclose information to the app. In fact, the trend in Figure 4.5a for younger adults was negative, which from a privacy calculus perspective would appear counter-intuitive. This finding suggests that younger adults may not value sharing more information for the purpose of personalizing financial recommendations to improve their credit score. A potential explanation for this outcome may be that younger adults have a relatively low financial literacy and are less attuned to their finances than older adults, as they are just starting to build their credit history [89, 52]. Therefore, impersonal recommendations may have seemed as useful to these participants as ones that were personalized to their financial situations.

In Figure 4.5b, I also see how younger adults rely heavily on the heuristic of app trust when evaluating the perceived sensitivity of the data being shared with the app.

From a heuristic perspective, it is plausible to argue that trusting the app will make younger adults feel safer and perceive less threat. Research shows that trust can function as a cognitive heuristic and guide individuals' risk perceptions [85, 189]. This seems to be the case here for younger adults who derive their sensitivity perceptions based on affect heuristic of trust. Emotions and heuristics act as mental shortcuts, whereby people access their pool of positive and negative feelings toward an issue to guide judgement [299]. On the other hand, older adults seem to consider data sensitivity as an inherent aspect of each data-item, and the level of trust does not significantly influence older adults' perceptions of data sensitivity. Furthermore, the risk-as-feeling hypothesis [198] suggests that emotional reactions to situations involving risk often block cognitive assessments of the situation and therefore heuristics drive such behavior. In this scenario, data sensitivity, which is significantly influenced by heuristics, was the only predictor for younger adults' disclosure decisions. In line with Worthy et al. 's [327] findings, the results suggest that younger adults' decisions are more driven by heuristics than older adults.

Furthermore, when taking into account that privacy is contextual, Nissenbaum's framework of contextual integrity [231] asserts that the recipient of the information (in this case, the CreditPush app) should be as important of a factor in assessing the appropriateness of information flows. Therefore, contextual integrity might also partially explain the heuristic decision-making process of younger adults. Similar to Miltgen and Peyrat-Guillard [222], who uncovered a "reversed" privacy paradox where younger adults expressed fewer privacy concerns but greater protective behaviors than older adults, I uncovered some interesting patterns among younger adults that seemed counter-intuitive to the privacy calculus framework but aligned with more heuristic decision-making processes. Therefore, I suggest additional research be conducted to further explore and unpack these relationships.

4.4.4 Implications for Design

A goal in privacy research is to help users make well-informed decisions. Some older adults believe that they are left out of the design process and not being attended to [109]. the results suggest that it is important to show older adults the value or benefits of sharing information online. If disclosure gratifications are not clearly identified, companies cannot simply rely on established relationships with older adults for them to be willing to share information. Traditional trust indicators like brand name may not be enough to reassure these users that disclosure is in their best interests. Efforts to design an app or website with outward signs of, e.g., reliability and trustworthiness may not be as effective as providing information on how and why disclosing will be beneficial. Nonetheless, for young adults, it may be vital to establish a trusting relationship that can make users feel more comfortable disclosing information.

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

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

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

4.5 Limitations and Future Work

Prior to concluding, I would like to highlight some of the limitations of this research and areas for future research. First, older adults are a heterogeneous group with different technical skills, physical, and cognitive conditions [121, 196] and I only recruited participants who passed cognitive tests, were familiar with computers, and had experience with internet and online platforms. This was important since previous research suggests that the cognitive load for older adults who are new to computer technology will be higher while performing different tasks, inhibiting their optimum performance [270]. For the same reason, I designed a web-based app to be simple. Since prior literature suggests privacy settings are difficult for older adults to locate and navigate through [50], the control mechanisms in this application were simple radio buttons (for choosing not to disclose) or text boxes (to enter information for disclosure). However, the recruitment strategy and the design of this app may limit the generalizability of the results to older adults who have experience with technology. Further research may also need to be done with applications that are designed with more complexity.

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

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

4.6 Conclusion

This chapter builds on the theoretical contributions of chapter 3, and studies privacy decisions using both privacy calculus and decision heuristics frameworks. Rather than focusing on *what* are the age-related differences in privacy, I focused on the *sources* of such differences. I studied the decision-making processes of younger and older adults in the context of a financial app. Using a dual-route privacy framework, I found that younger adults heavily rely on heuristics, whereas older adults are more likely to be calculus-driven thinkers. However, the heuristics impacted younger adults' decision-making in an unexpected way; rather than directly impacting disclosure, reliance on heuristics actually altered the perceived sensitivity of various pieces of personal information. Understanding these underlying mechanisms of privacy decisions can inform the design of digital products and help product developers and designers better support their various users' diverse privacy decision-making processes. In the next chapter, I discuss how current design practices put older adults at a disadvantage by making them susceptible to over disclosure.

Chapter 5

Practices in Platform Designs Put Older Adults at a Disadvantage

Online websites often use dark patterns to increase users' information disclosure. Common examples include "opt-out" privacy defaults, positive framing, and positive justification messages encouraging disclosure behavior. In Chapter 4 I showed that older adults undergo a different privacy decision-making process compared to younger adults. However, more research is needed to show the attitudinal (privacy concerns in the scope of this chapter) and behavioral (disclosure behavior) effects of these strategies for different age groups. To address this gap, I re-analyzed the dataset discussed in Chapter 3 while limiting my inclusion criteria to older (above 65 years old, N=44) [57] and young adults (18 to 25 years old, N=162) [229, 239]. I also draw from dark pattern literature and present the manipulations as common dark pattern design strategies: framing (positive vs. negative), privacy defaults (opt-in vs. opt-out), and justification messages (positive normative, negative normative, positive rationale, negative rationale, none).

Therefore, this chapter contributes to the literature by addressing the following research questions:

RQ1*: What are the effects of dark pattern designs on users' attitudes and behaviors?*

RQ2*: How do older adults react differently than young adults to dark pattern designs in terms of their attitudes and behaviors?*

Overall, the results of my analyses show support for the effectiveness of dark pattern designs in the sense that positive framing and opt-out privacy defaults significantly increased disclosure behavior, while negative justification messages significantly decreased privacy concerns. Regarding older adults, the results show that certain dark patterns do lead to more disclosure than for younger adults, but also to increased privacy concerns for older adults than for younger. However, there was no influence of these concerns on disclosure, and instead, they are outweighed by the pro-disclosure effects of dark patterns. This suggests that privacy concerns may not be a sufficient force to drive individuals to act on protecting their privacy when in the presence of dark patterns and that such patterns may be even more dangerous for older users.

5.1 Background

In this section I discuss dark pattern designs and common strategies to maximize users' disclosure (namely framing, defaults, and justification messages).

5.1.1 Dark Pattern Designs

Dark patterns in design refer to instances where designers exploit human desires and behaviors and implement functionality that will mislead them and have negative implications [127]. The term was first proposed by UX designer Harry Brignull in 2010, who defined dark patterns as: "a user interface that has been carefully crafted to trick users into doing things they might not otherwise do. "Brignull also notes that "Dark patterns are not mistakes. They are carefully crafted with a solid understanding of human psychology, and they do not have the user's interests in mind." [127]. Bösch et. al developed a categorization of privacy dark patterns that designers implement within their systems to exploit the users' privacy. These strategies include: maximize, publish, centralize, preserve, obscure, deny, violate, and fake [48].

In the context of this work, I focus on the *maximize* dark strategy by which designers aim to collect more data than is actually needed for the task [48]. Framing, defaults, and justification messages are means by which these designers maximize the amount of personal data collected [48, 211, 150]. I study these dark patterns in the context of a Facebook application—a context in which dark patterns are not uncommon. For example, in the infamous Cambridge Analytica case, the app designers used maximize dark pattern designs to maximize disclosure. The app used defaults to influence users' decisions to share personal information with rather unfavorable consequences. In this study, I test the effect of dark patterns in the context of a photo-tagging application on the Facebook platform where users can choose to tag themselves or their friends in their photos. The app applied maximize dark pattern designs to influence the user's decision in the form of choice framing, default settings, and justification messages. Below, I explain each of these maximize dark patterns.

5.1.1.1 Framing and Defaults

Framing and defaults are quintessential examples of the "maximize" dark pattern, in that they tend to increase compliance to disclosure requests made by the information system [22]. The framing effect describes the phenomenon that people are more likely to give consent to a request if it is presented with a positive framing ("Do ...") rather than a negative framing ("Do not ..."). Johnson et al. [146] and Lai and hui [179] independently studied the framing effect in the context of information privacy. At the end of an online health survey, Johnson et al. [146] asked their participants if they wanted to receive more health surveys. The wording of the choice option for participants in the positive framing condition was "Notify me about more health surveys", whereas those in a negative framing condition saw the choice wording as "Do not notify me about more health surveys". Lai and Hui [179] studied framing in a newsletter sign-up scenario. Similarly, the wording for their positive framing condition was "Please send me Vortrex Newsletters and information" whereas the wording for the negative framing condition was "Please do not send me Vortrex Newsletters and information". Both Johnson and Lai and Hui found that participants are more likely to comply with the request if the request is presented with a positive framing rather than a negative framing.

Similar to framing, defaults are a form of dark pattern design strategy that can influence individuals' decisions [150, 263]. The default effect suggests that individuals are more likely to accept an option if that option is pre-selected by default [264]. This is evident in both Johnson et al. [146]'s health survey study and Lai and Hui [179]'s newsletter sign-up study, where sign-up ratio is highest if users are signed up by default (an opt-out default). Overall, both framing and defaults are referred to as tools of choice architecture [150] which can induce compliance to data disclosure requests made by the information system [22].

5.1.1.2 Justification Messages

To help users make a decision, system designers sometimes show them justification messages[1] providing additional information about the choice. These messages can inform users about the popularity of the product or service among other users [103] or its pros and cons [111, 48]. For example, Weinberger et al. [317] show that an unfavorable product rating adversely influences individuals' intention to purchase the product. Overall, these studies suggest that providing justifications supporting a request would motivate the audiences to comply to the request.

5.2 Theoretical Framework

In the sections below, I present information disclosure and privacy concerns as the two outcome variables of interest when examining the influence of dark-pattern designs. As this chapter is a secondary analysis of the data dsicussed in Chapter 3, I will not discuss the methods section again. Figure 5.1 shows the hypotheses via the research model. I investigate these hypotheses using a path model. In a path model, variables can function as both dependant variables (DVs) and independent variables (IVs). In this case, privacy concerns is a DV where I study the effects of dark pattern designs on it, and is an IV when I study how it predicts disclosure behaviors.

5.2.1 Disclosure Behavior

Oversharing information on social media can lead to negative consequences for users [260]. Therefore, social media platform users employ a wide range of privacy management strategies to manage their interpersonal boundaries, such as managing their relationship boundaries (e.g., by adding a new friend or unfriending someone) and their territorial boundaries (e.g., by tagging or untagging oneself or someone else in/from photos) [323]. Existing literature regards tagging as a form of disclosure [324], since photo tagging can reveal the tagged person's online information (e.g. name, social media page) to a broader audience when the photo is shown on friends' timelines. Tagging other people in ones' photos is a contentious issue [324]: on the one hand, it can increase group cohesion and build social capital [216, 262], but on the other hand, it can lead to an interpersonal

[1] The term "framing" is used in the literature to denote several conceptually distinct interventions, and some studies apply the term "framing" to the type of justifications I used in this study [45]. In order to avoid confusion, I use the term "framing" for negated choice statements (i.e., "Do" vs. "Do not"; [179, 146]), and the term "justification" to refer to the additional text accompanying the choice statement.

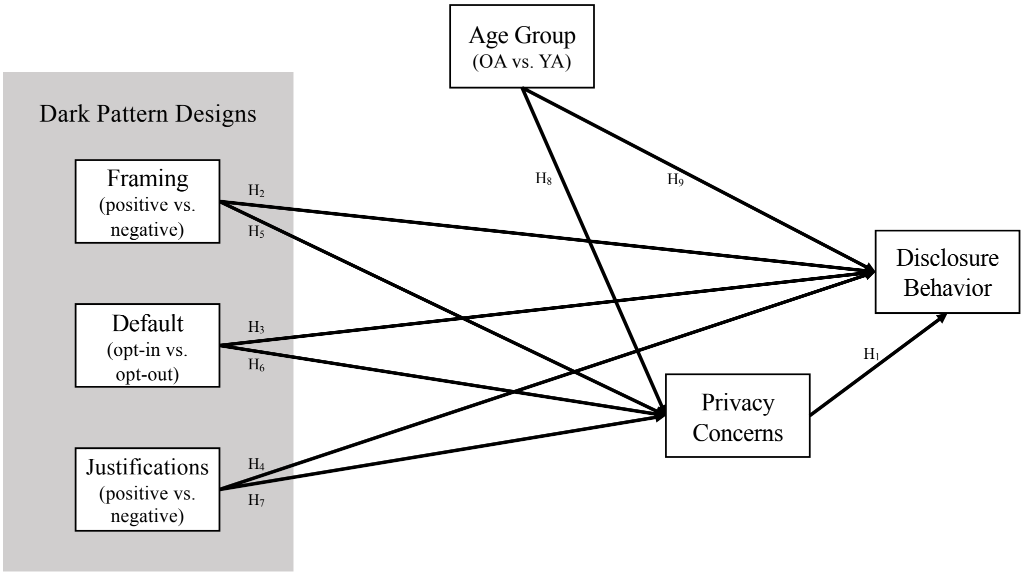


Figure 5.1: Research model and the age-related effects of dark-pattern designs on privacy concerns and disclosure behavior (OA: older adults, YA: young adults).

privacy violation if the others prefer not to be tagged [125, 286].

5.2.2 Privacy Concerns

The privacy literature has not reached a consensus about the relationship between privacy concerns and disclosure behaviors. On the one hand, many studies suggest a negative association between privacy concerns and disclosure behaviors [151, 277, 100]. The general argument in these studies is that a high concern for privacy motivates individuals to refrain from disclosing their data. On the other hand, many studies have found that despite their high privacy concerns, individuals freely give up their personal information—a phenomenon that is so prominent that it has been dubbed the "privacy paradox" [38]. The privacy paradox suggests that privacy concerns have little or no relationship with self-reported or observed disclosure behaviors [291, 218, 282]. For example, Tufekci [302] studied students' self-reported disclosure behaviors on social network sites. Her results show "little to no relationship" between online privacy concerns and disclosure on online social network sites. Despite these contradictory findings, I pose the following hypothesis reflecting the base expectation that privacy concerns are predictive of disclosure behaviors:

H1: *Individuals with higher privacy concerns are less likely to disclose.*

In the following two sub-sections, I build on the RQ1 by posing six hypotheses about the relationships between dark pattern design, disclosure behavior, and privacy concern. I then address the RQ2 by posing two hypotheses regarding the effect of age on disclosure behavior and privacy concerns.

5.2.3 Behavioral Effects of Dark Pattern Designs: Inducing Disclosure

In this section, I discuss the behavioral effects of framing, defaults, and justification messages. Particularly, I draw upon the "privacy dark patterns" literature to hypothesize how these design features are being used to increase disclosure.

5.2.3.1 Framing and Defaults

Framing and default effects have been extensively studied in the privacy domain. Johnson et al. [146] and Lai and Hui [179] independently found framing and default effects to have a significant impact on users' decisions. In both studies, a positive framing and an opt-out default setting increased the likelihood of users accepting the disclosure requests. In line with these findings, I study two conditions of framing (positive - "tag me in the photos" vs. negative - "do not tag me in the photos"), and two conditions of the default (opt-out vs. opt-in). I hypothesize the following:

H2: *A positive framing will increase disclosure.*

H3: *An opt-out default will increase disclosure.*

5.2.3.2 Justification Messages

Existing literature suggests that prompting individuals with a message about a product or service can influence their decisions in favor of the message content [192, 126, 164, 316]. Dark pattern designs sometimes use this feature to promote disclosure [48, 211]. For example, they show messages about a product's popularity in the form of reviews [91] which can sometimes be fake and misleading [285, 309, 292]. Hanson and Putler [126] showed participants a normative justification: an arbitrary integer ostensibly representing the number of downloads of a software program. Participants who saw a higher number were more likely to download the software for themselves. This is arguably due to a herding effect [26], where individuals follow the footsteps of the majority. In addition to such normative justifications, dark pattern designs sometimes use descriptive justification—pushing the benefits of the product—to promote product use or disclosure [48, 211]. For example, in the context of a travel advisor app, designers prompted users with a message of “by signing in, you can download over 300 cities, locations, and reviews to your phone” [48]. Reading about the benefits of the product is arguably a motivating message to sign in and use the app. Having higher quality reviews will increase the likelihood of one buying an online product [164], or talking about the effectiveness (pros) of treatment rather than the cons will increase the likelihood of accepting it [45]. In line with these findings, I study five conditions of justification messages (positive/negative normative, positive/negative rationale-based, none). I pose the following hypothesis:

H4: *Positive (as opposed to negative) justification messages will increase disclosure.*

5.2.4 Attitudinal Effects of Dark Pattern Designs: Inducing Concerns

The effects of framing, defaults, and justification messages on disclosure behavior are evident in the literature [150, 9, 179, 23, 146, 126]. The compliance-inducing effects of such design interventions meet the goal of dark pattern designs. However, research shows that the behavioral effects of these dark pattern strategies may not actually map to their attitudinal effects [29, 162, 169]. In this section, I examine the effects of dark pattern designs on individuals’ state of privacy concerns. Privacy concerns are often measured as an individual trait, rather than a dynamic state [277]. However, this assumption may not be valid. Few studies consider privacy concerns as a dynamic state [261]. This chapter further contributes to the literature by highlighting this perspective and presenting privacy concerns as a dynamic state which can change in response to different design strategies.

5.2.4.1 Framing and Defaults

Online firms have an incentive to collect as much data about their users as they can. Data is an important asset in the industry [140, 49, 281]. For example, having data about customers’ preferences and needs can help firms better target their advertisements to individuals likely to need their product and avoid the unnecessary costs of contacting consumers whose preferences do not match the product [140]. Therefore, some companies adopt dark-pattern design strategies to collect more user data [48].

Framing and default are compliance-inducing mechanisms [22] that are often used in dark pattern designs [211, 210, 120]. Dark pattern default options are designed to encourage sharing of personal information and to maximize online firms’ collected data [48]. Likewise, dark pattern designs use positive framing in the choice statements to endorse disclosure [211]. Whereas the behavioral effect of such dark pattern designs are outlined in Section 5.2.3, here I note how these interventions can adversely influence users' attitudes towards the system [48, 201]. For instance, Knijnenburg and Kobsa [169] found that an opt-out default would increase perceived oversharing threats compared to an opt-in default. Therefore, I pose the following hypothesis:

H5: *A positive framing will increase privacy concerns.*

H6: *An opt-out default will increase privacy concerns.*

5.2.4.2 Justification Messages

In the context of dark-pattern design, I argue that while a positive justification message might be intended to encourage individuals to use an app or increase disclosure, it could also increase users' privacy concerns, especially when they realize that the justification message is used as a dark-pattern strategy. Conversely, users may find a negative justification (i.e., cautioning them about the cons of the product) a sincere message [162] that is indicative of the developer's benevolence and/or integrity (two of the primary components of trust [214]). For example, communicating potential risks in a study report will increase its perceived trustworthiness [273]. Since trust and privacy concerns are inter-related [95], I argue that a negative justification will result in lower privacy concerns:

H7: *Negative (as opposed to positive) justification messages will decrease privacy concerns.*

Next, I explain the effects relating to age and the second research question.

5.2.5 Examining Differences between Older Adults and Young Adults

Literature suggests a positive association between age and privacy concerns, indicating higher concerns for older users [307]. However, the literature shows mixed findings in terms of the main effect of age on disclosure behaviors. While some studies do not report a significant relationship between age and disclosure [153], other studies show higher disclosure rates for older adults [272]. Despite these mixed findings, I pose the following hypotheses to investigate these effect:

H8: *Older adults will have higher levels of privacy concerns than young adults.*

H9: *Older adults will disclose more information than young adults.*

To the best of my knowledge, this study is the first to investigate the difference between older and younger adults responses to the dark pattern designs.

5.3 Research Methods

This chapter uses the existing dataset from Chapter 3. Therefore, please refer to Chapter 3 to see details on the experimental setup. In addition to variables explained in Chapter 3, this chapter also analyzes a reduced version of the IUIPC [205] dimension of general concerns with 3 items. This reduced version is validated and used in the previous studies [168]. I used the sum score of this scale for measuring privacy concerns (Cronbach's $\alpha = 0.790$). All the items were measured on a 5-point agreeableness Likert scale:

- Compared to others, I am more sensitive about the way online companies handle my personal information.
- To me, it is the most important thing to keep my privacy intact from online companies.
- I am concerned about threats to my personal privacy today.

I standardized the scale (grand mean = 0, SD = 1) in the analyses.

5.3.1 Data Analysis Approach

The first dependant variable (decision) was a binary variable with "accept to tag" coded as 1 and "reject to tag" coded as 0. Each participant responded to six disclosure scenarios: three scenarios on whether they wanted to tag themselves in each of their three friends' photos and three scenarios on whether they wanted to tag each of their three friends in their own photos. Therefore, I constructed a multilevel path model with a random intercept to account for repeated measures per participant and a binary dependent variable. The path model enabled me to treat privacy concerns as both an independent variable (by regressing tagging decision on it) and a dependent variable (by regressing it on study manipulations). The framing and default manipulations were dummy-coded where positive framing or opt-out defaults were coded as "0.5" and negative framing or opt-in defaults were coded as "−0.5". To analyze justification messages, I first conducted an overall chi-square omnibus test to study their overall effect among the 5 conditions. Then I ran planned contrasts, including a contrast testing the effect of justification valence (positive justifications vs. negative justifications) to study H4 and H7. The other contrasts tested the effect of any justification (no vs. any), the effect of the type of justification (rationale-based vs. normative), and the interaction between justification type and valence). The analyses were carried out in Mplus v7.4. As the sample was imbalanced (44 older

Table 5.1: An overview of the study's results regarding the hypotheses

Hypothesis	**Support**
H1: High privacy concerns –> Low disclosure	Not supported
H2: Positive framing (vs. negative) –> High disclosure	**Supported**
H3: Opt-out default (vs. opt-in) –> High disclosure	**Supported**
H4: Positive (vs. negative) justifications –> High disclosure	Not supported
H5: Positive (vs. negative) framing –> High privacy concerns	Not supported
H6: Opt-out (vs. opt-in) default –> High privacy concerns	Not supported
H7: Negative (vs. positive) justifications –> Low privacy concerns	**Supported**
H8: Older adults (vs. younger adults) –> High concerns	Not supported
H9: Older adults (vs. younger adults) –> High disclosure	**Supported**

adults and 169 young adults), I used MLR, a maximum likelihood estimation with robust standard errors in the analyses [225].

5.4 Results

5.4.1 Sample Characteristics

Across the older adult participants, there were 15 females and 29 males. Their average age was 68.8 years (min = 65, max = 77, sd = 3.23). The young adult sample had 87 males, 71 females, and 4 individuals who did not self-identify as female or male. Their average age was 20.30 (min = 18, max = 25, sd = 2.18). The dataset also measured participants' Facebook usage frequency on a 9-point scale from "Never" coded as 0 to "Almost constantly" coded as 9 and the time they spend on Facebook in each session on a 5-point scale from "A few minutes" coded as 1 to "Several hours" coded as 6. On average, older adults used the Facebook platform more frequently (mean = 5.708, sd = 1.519) compared to younger adults (mean = 5.402, sd = 2.055). However, both age groups spent an average time of 30 minutes on Facebook (older adults: mean = 2.054, sd = 1,194 and young adults: mean = 2.119, sd = 1.275). In the following, I present the analyses with regards to the hypotheses. Table 5.1 summarizes the hypothesis tests.

5.4.2 Effects on Tagging Decision

In contrast to H1 and in line with the privacy paradox, the results did not suggest any significant relationship between privacy concerns and disclosure decision ($p > .05$). Therefore, H1 is rejected. However, I found support for H2 and H3 suggesting both framing and default significantly

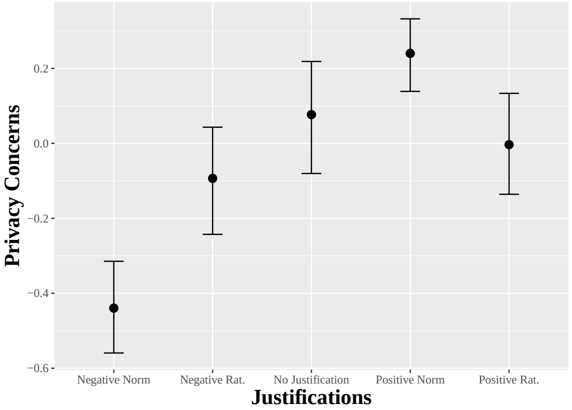


Figure 5.2: The y-axis is standardized sum-score of privacy concerns. The graph shows that negative justifications lead to lower levels of privacy concerns.

influence tagging decisions. Users who see the positively framed option of "Tag me in the photos" were 31.9% more likely [2] to use the tagging feature compared to those who see the negatively framed option of "Do not tag me in the photos" ($p < .001$). Furthermore, those users who were being tagged by default were 19.4% more likely to use the tagging feature ($p < .01$). In addition, in contrast to H4, the various justifications did not influence tagging decision differently ($\chi^2(4) = 0.823, p > 0.05$). Finally, in line with what I hypothesized in H9, older adults were 19.8% more likely to use the tagging feature compared to young adults ($p < .05$).

5.4.3 Effects on Privacy Concerns

In contrast to H5 and H6, the results did not suggest any significant effects of framing and default manipulations on privacy concerns ($p > .05$). However, I did find a significant main effect of justifications on privacy concerns ($\chi^2(4) = 9.827, p < 0.05$). Subsequent planned contrast tests revealed a significant effect of justification valence ($p < 0.05$), supporting H7 and suggesting that negative justification messages lower users' privacy concerns compared to positive justifications by 0.132 standard deviations. However, this effect was negated by a marginal interaction between justification type and valence, meaning that the difference between positive and negative justifications mostly hold for normative justifications (see Figure 5.2). Finally, in contrast to H8, older and younger adults did not have significant differences in terms of their overall level of privacy concerns

[2] To present the results in a comprehensive manner, I convert the log odds-ratio to percentages. For example, the effect of framing on disclosure is 0.277 (Table 5.2), which is a log odds-ratio. Therefore, disclosure in the positive framing group is $e^0.277 = 1.319$ times higher than in the negative framing group, i.e., a 31.9% difference in the odds of disclosure

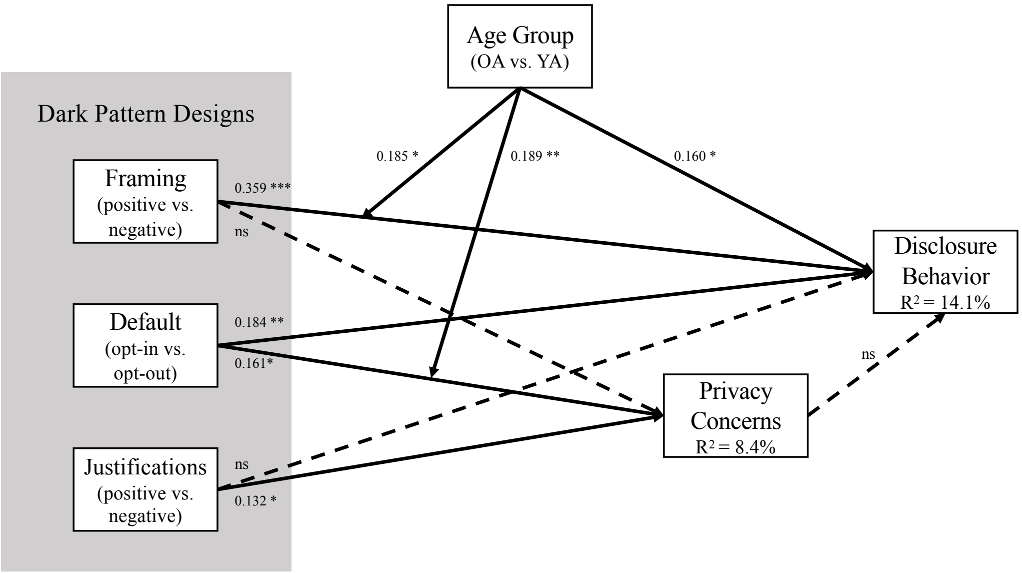


Figure 5.3: The results of the saturated path model including all of the significant findings (ns: not significant hypotheses, * p < .05, ** p < .01, *** p < .001)

($p > 0.05$).

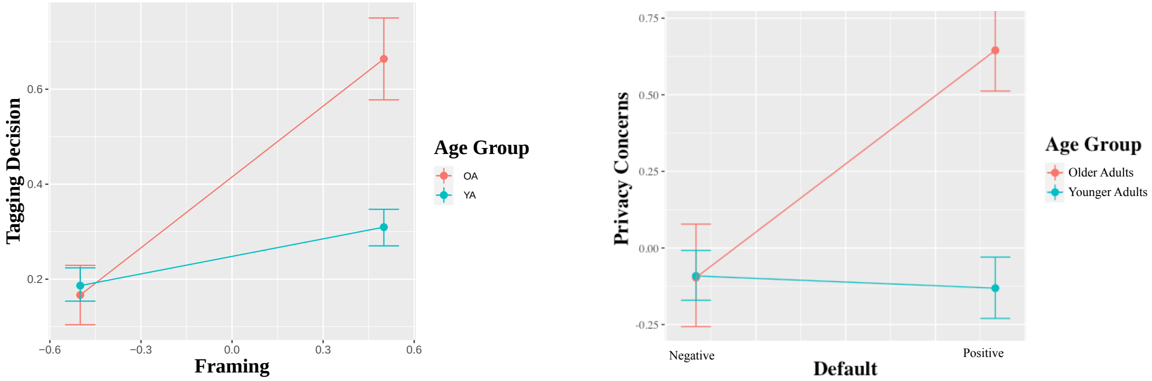
These results show that in contrast to H8, older and younger adults have the same levels of privacy concerns. Furthermore, while having the same levels of concern, older adults are more open to disclosure. I further unpack the effects of age by studying moderation effects of age and dark pattern designs. Therefore, I run a saturated path model and report it below. Figure 5.3 and Table 5.2 summarize the results.

5.4.4 Moderating Effects of Age Group on Tagging Decision

The results show that the age group moderates the effect of framing on tagging decision. The effect of framing was stronger for older adults than for young adults: older adults who were exposed to a positively framed option were 53.1% more likely to use the tagging feature while young adults who were exposed to a positively framed option were only 33.1% more likely to use the tagging feature ($p < .05$). Figure 5.4a depicts this effect. The results show a similar moderation effect for defaults suggesting that older adults were more likely to keep the default option and use the tagging feature compared to young adults. However, this effect did not reach significance ($p = .062$). Similarly, age did not moderate the effect of justifications on the tagging decision ($\chi^2(4) = 4.822, p > 0.05$). Lastly,

Table 5.2: summary of the results. Odds Ratios (OR) are calculated for the tagging decisions where the outcome variable is binomial. Standard errors (SE) and beta coefficients (b) are also presented.

Variables	b (OR)	SE	p
DV: Tagging Decision			
Age Group (OA vs. YA, H9)	**0.160 (1.173) ***	**0.073**	**.028**
Privacy Concerns (H1)	0.049 (1.050)	0.087	.573
Framing (pos vs. neg, H2)	**0.359 (1.431) *****	**0.079**	**.0001**
Default (pos vs. neg, H3)	**0.184 (1.202) ****	**0.070**	**.009**
Justifications	$\chi^2(4) = 1.402$		.843
No vs. Any	-0.047 (0.954)	0.080	.559
Negative vs. Positive (H4)	-0.030 (0.970)	0.078	.706
Normative vs. Rationale	0.058 (1.059)	0.078	.461
Justification type X Valence	0.033 (1.033)	0.081	.686
Age Group X Privacy Concerns	-0.136 (0.872)	0.110	.216
Age Group X Framing	**0.185 (1.203) ***	**0.082**	**.029**
Age Group X Default	0.189 (1.208)	0.101	.062
Age Group X Justifications	$\chi^2(4) = 4.822$		.306
No vs. Any	-0.022 (0.978)	0.104	.833
Negative vs. Positive	-0.064 (0.938)	0.086	.454
Normative vs. Rationale	-0.158 (0.853)	0.079	.046
Justification type X Valence	-0.089 (0.914)	0.087	.306
DV: Privacy Concerns			
Age Group (OA vs. YA, H8)	0.093	0.059	.117
Framing (pos vs. neg, H5)	-0.013	0.078	.867
Default (pos vs. neg, H6)	**0.161**	**0.071**	**.024**
Justifications	**$\chi^2(4) = 10.133$**		**.038**
No vs. Any	-0.038	0.072	.600
Negative vs. Positive (H7)	**0.132 ***	**0.065**	**.042**
Normative vs. Rationale	0.040	0.067	.551
Justification type X Valence	**-0.131 ***	**0.066**	**.046**
Age Group X Framing	0.008	0.072	.913
Age Group X Default	**0.189 ****	**0.070**	**.007**
Age Group X Justifications	$\chi^2(4) = 3.707$		.447
No vs. Any	0.070	0.057	.217
Negative vs. Positive	0.097	0.076	.207
Normative vs. Rationale	0.042	0.079	.597
Justification type X Valence	0.008	0.079	.921



(a) The y-axis shows the actual tagging decision with zero as reject and one as accept. The graph shows that a positive framing is a more effective dark pattern strategy for older adults in terms of inducing disclosure.

(b) An opt-out default can increase older adults' concerns for privacy

Figure 5.4: The effects of framing and defaults on privacy concerns and privacy decisiosn

while the effect of privacy concerns on the tagging decision was stronger for older adults than for young adults, this effect was not significant ($p > .05$).

5.4.5 Moderating Effects of Age Group on Privacy Concern

The effect of defaults on privacy concerns were moderated by age group: an opt-out default increased older adults privacy concerns by 0.255 times standard deviation compared to a negative default, while an opt-out default increased young adults' privacy concerns by only 0.066 times standard deviation compared to a negative default ($p < 0.01$). Figure 5.4b depicts this effect and suggests that an opt-out default only significantly increases the privacy concerns for older adults. Age group did not moderate the effects of any other variable on privacy concerns($p > 0.05$).

5.5 Discussion

In this section, I first discuss the main effects of dark pattern design strategies on users' disclosures and privacy concerns (RQ1). I then discuss how dark pattern designs influence older adults differently compared to younger adults (RQ2). Finally, I conclude the discussion section by presenting the design implications of this work.

5.5.1 The Impact of Dark Pattern Designs on Disclosure Behaviors

In this study, I did not find support for H1 and therefore did not find privacy concerns significantly influence the tagging decision. This finding confirms the privacy paradox theory that individuals' disclosure behaviors are not necessarily in-line with their self-reported privacy concerns [38]. However, I should consider that the effect of privacy concerns on disclosure was not studied in isolation. The framing and default nudges were also present in the decision scenario which, indeed, significantly influenced users' decisions (H2, H3). It is possible that concern for privacy was not a determining factor for users in the presence of such dark pattern design interventions. As an implication of RQ1, future studies should focus more on dark pattern designs, even more so than privacy concerns, as dark pattern designs have a stronger effect on users' disclosure behaviors. The results show that even raising privacy concern does not translate to privacy protective behaviors.

5.5.2 The Impact of Dark Pattern Designs on Privacy Concern

Despite many privacy frameworks depicting privacy concerns as a dynamic and very fluid concept [240, 231, 18], the majority of the privacy literature has studied privacy concerns as a static variable predicting disclosure [277, 330]. This study considers privacy concerns as a dynamic result of design patterns. The results suggest that concern for privacy is not necessarily a static trait, and rather can change in response to the design patterns. Specifically, negative justifications can decrease users' privacy concerns. A possible explanation is that showing a negative justification makes users feel that the app is more sincere. This , in turn, lowers levels of privacy concern. For example, showing a negative normative justification is an indication of low popularity of a product and is an uncommon practice and induces lowers levels of privacy concern.

5.5.3 Dark Pattern Designs May Disproportionately and Negatively Impact Older Adults

In terms of RQ2, I studied the the difference between older and younger adults privacy concerns and disclosures. In addition, I studied the moderating effects of age. While older and younger adults had similar privacy concerns, the results show that an opt-out default dark pattern alerts older adult users and makes them privacy-cautious. Using opt-out defaults is one of the most common means of data collection by firms [146]. It is possible that the older adult participants had more experience and familiarity with the default mechanisms and, therefore, an opt-out default led them to be more privacy-cautious.

With regards to the effects of age on tagging decisions, the results suggest that older adults were more likely to use the tagging feature. This is in-line with some previous findings in the literature on older adults disclosing more data [272]. In addition to this main effect of age on decision, I found that the framing effect is a stronger nudge in pushing older adults to use the tagging feature when compared to younger adults. Likewise, I found opt-out defaults to be a stronger nudge for older adult participants; however, the moderation effect with defaults did not reach the significant thresholds ($p = 0.062$). These effects may be explained by the literature on loss-aversion. Losses are weighed more heavily than gains and so individuals put forth more effort to avoid losses than to acquire gains [304, 305]. An opt-out default can trigger an instant endowment for the user, where the tagging disclosure is seen as something they have [96, 206]. Therefore, changing the default is being perceived as a loss and individuals are more likely to keep the default option [155, 156]. Likewise, a positive framing endows individuals with the benefits of disclosure, but foregoing disclosure is perceived as a loss [146, 149]. This is further supported by the psychology literature which suggests that older adults are generally more loss-adverse than young adults [209, 92, 147, 61]. Scholars have found that older adults are willing to take more risks [209] or exert more effort [61] to avoid a loss, in comparison with young adults. Therefore, the framing and default manipulations triggered a loss-aversion process which influenced older adults more than younger adults.

5.5.4 Implications for Design

This study has several design implications. A key finding is that while using opt-out defaults increases older adults' privacy concerns, it still ends up increasing their disclosure levels. This goes counter to the common perception about older adults having low privacy awareness, since they identify an opt-out dark pattern design—even more so than younger adults—and become privacy-cautious. However, these dark pattern interventions had stronger behavioral effects than any heightened privacy concerns. Therefore, instead of efforts to make individuals privacy-cautious and increase individuals' privacy concerns, hoping for them to take privacy protective measures, it may be more effective to focus on how to counter dark design patterns. This might even include developing policies that discourage or regulate the use of dark design patterns.

This study also shows that older adults may be more amenable to framing and default nudges due to their loss-aversive nature. This result is a call to technology developers to be mindful of their older adult audiences and take on the ethical responsibility of creating technologies that avoid such nudges. In fact, prior research suggests that older adults may choose not to use technology as a result of high privacy concerns [171]. While the opt-out default increased disclosure in this study, it is conceivable that having to make a plethora of loss-aversive decisions could push privacy concerns beyond a threshold where older adults decide to stop using technology altogether. Further research is needed to investigate this, but in the meantime, product designers should be conscientious towards their older adult users and not increase their concerns.

Finally, while it may seem counter intuitive, if product designers are honest about the negative aspects of their product, specially the low adoption of their features, it may actually alleviate concerns. The negative justifications manipulation proved to reduce privacy concerns. Being honest seems to be the best policy for gaining consumer confidence.

5.6 Limitations and Future Work

While this study was able to investigate both older and younger adults and gain insight into how dark patterns differently affect these age groups, it was an initial exploration with a non representative sample. Future research should study this phenomenon with a bigger sample of participants that are balanced to be representative. Also, since privacy is a culturally-shaped construct, investigating attitudes in other cultures and countries would broaden our understanding beyond the United States. Furthermore, this chapter studied disclosure behaviors in the context of tagging on social media. The effect of these patterns may vary in different contexts. Thus, future research should consider privacy decisions made in context of other domains such as for e-commerce or healthcare services.

5.7 Conclusion

This chapter studied the attitudinal and behavioral impact of dark pattern designs on older and younger adults. While an individual's levels of privacy concerns may change in response to these design strategies, the behavioral effects of such strategies are dominant and individuals still end up disclosing their data despite heightened concerns. Furthermore, while older adults respond with more concern to some of these dark pattern designs than young adults, they are actually more vulnerable to such design strategies, perhaps due to a loss-aversive nature. Therefore, policy designers and technology developers should become familiar with the unique privacy attitudes and behaviors of older adults when it comes to disclosure. The solution may be a combination of identifying technology designs that counter the effects of dark patterns, as well as establishing rules and regulations around their use. Until that happens, older adults may continue to be disproportionately affected by dark pattern designs.

Chapter 6

Investigating the Role of Privacy Literacy, Self-efficacy, and Concerns in Older and Younger Adults' Privacy Decisions

Chapter 4 shows that older and younger adults have different thinking mechanisms when making privacy decisions. When interacting with a financial recommender application, older adults are more likely to be privacy calculus-driven thinkers than younger adults. On the other hand, younger adults proved to rely on heuristics more than older adults. The current gap in these findings is that they do not discuss any variables that may have led to this difference. Previous studies only ascribe the difference between older and younger adults thinking mechanisms to their age gap. However, age in and of itself may not be the fundamental reason for this difference, and there may be hidden variables causing this difference. I will attempt to uncover such variables in this chapter.

Privacy literacy, privacy self-efficacy, and privacy concerns are essential parameters when studying the privacy of the older adult population. Scholars speculate that lack of privacy literacy and self-efficacy leads to higher privacy risks for senior citizens and is one of the deterrent factors that preclude older adults from using technology products [107, 301, 250]. Interacting more with technology does not necessarily improve the situation. For example, older adults maintain a low self-efficacy related to technology, even after long-term usage of technology products [321]. Arguably, older adults who believe they cannot manage their online privacy also feel more worried about their privacy. Indeed, research shows that older individuals have higher levels of privacy concerns than younger age groups [307]. Therefore, the difference in decision-making mechanisms between older and younger adults may result from having different levels of privacy literacy, privacy self-efficacy, and privacy concerns. I attempt to close this gap by studying whether and how privacy literacy, self-efficacy, and concerns account for the difference between older and younger adults' privacy decision-making mechanisms.

Drawing on the conceptual model I outlined in chapter 2, and the results of chapter 4, I used the dual-route privacy framework to study older adults' privacy decisions and compare it to younger adults'. For this study, I specifically used the Elaboration Likelihood Model (ELM) [247, 246]. This model was initially developed to show different ways of processing a message (as stimuli) and predict the persuasive effects of the message (whether it can change an individual's attitudes). However, scholars adopted the ELM to a wide range of tasks [246] including privacy decision making [313, 36]. The ELM suggests that individuals process the stimuli through two major routes: the central route and the peripheral route. The decisions made through the central route are highly elaborated and require more cognitive effort. The central route corresponds to the privacy calculus, as both represent a rationalistic decision. On the contrary, the decisions made by the peripheral route are less elaborated and require less cognitive effort, similar to heuristic decisions. The ELM notes two prerequisites for a decision to be processed through the central route. Without these two requisites, elaboration is not very likely, and individuals may use the peripheral route to make decisions instead. The first requisite is the decision maker's ability to process the information relating to the decision task. An individual who lacks issue-specific knowledge about a topic cannot ponder upon it and make an elaborated decision unless they gain the knowledge. However, the elaboration is more likely when an individual can process the stimuli. The second requisite is an individual's motivation about the issue. The decision-maker may elaborate a decision if they are motivated to do so. On the contrary, an individual who lacks the motivation to ponder upon a decision is not likely to invest cognitive effort on the topic and will use the less effortful peripheral route.

In this study, I designed an experiment with both heuristic and cognitive manipulations.

The heuristic manipulations evaluate the two groups' tendencies to follow a decision shortcut (i.e., peripheral route in the ELM). The first heuristic manipulation was the endowment effect, presented in neutral (i.e., choice), privacy endowed, and service endowed conditions. The second heuristic manipulation was a disclosure nudge that highlighted the option encouraging disclosure. Furthermore, I designed cognitive manipulations serving as rational cues to trigger different risk/benefit assessments within the privacy calculus framework (i.e., the central route in the ELM).My dual-route privacy framework specifically informs this design. The heuristic manipulations measure individuals' tendencies to follow the peripheral route and make heuristic decisions. In contrast, the rationale manipulations measure individuals' preferences to follow the central route and subject their decisions to the privacy calculus.

In the following, I discuss the related work and the operationalization of the study. Then, I report the expected results and discuss the implications of my findings.

6.1 Theoretical Background and Hypothesis Development

6.1.1 Endowment Effect, a Heuristic Byproduct

The endowment effect is a decision heuristic referring to the phenomenon in which people are reluctant to abandon their belongings even if a better or worthier case is offered [156]. Research finds evidence of endowment effect on individuals' privacy valuations [8]. Acquisti et al. [8] conducted a field study in a grocery store; they gave some participants a \$10 anonymous gift card. After that, they offered to exchange the \$10 anonymous card with a \$12 identified gift card. The \$12 gift card was of a higher value by \$2, but it was identified so that the card holders' name was linked to the transactions completed with the card. The procedure was reversed for other participants; they first received the \$12 identified gift card and were given a chance to exchange it with a \$10 anonymous gift card. The results show that more than half of participants who were first given the \$10 anonymous gift card chose to proceed with the \$10 gift card. However, only about ten percent of the participants who initially got the identified \$12 gift card chose to switch to the \$10 anonymous gift card. Some of the participants in this study were neither endowed with the identified nor the private gift cards. Instead, they could choose between the two cards (i.e., the neutral or choice condition). %35 of these participants chose to have the \$10 anonymous gift card, and the rest of them chose the \$12 identified card. These findings show that individuals' decisions can be influenced by whether they are endowed with their privacy or with an additional monetary reward.

While Aquisti et al.[8]'s study is concerned with physical gift cards, I move the concept of endowment into the digital world altogether. In the physical world, there is a tangible physical commodity. This may not necessarily be true in the case of the digital environments where users own their data, but they can disclose it in return for some services. A great example is a GPS navigation app that can work by disclosing location data. In the scope of the endowment heuristic, one may start using an e-map with location data being kept private (privacy-endowed) but, inevitably, will not be able to use the GPS navigation without disclosing the real-time location. On the other hand, one may start using the app with GPS service being enabled (service endowed) but, inevitably, will not have location privacy without disabling the live tracking. Based on the endowment literature, I pose the following hypothesis:

H1a: *Those who are endowed with their privacy are less likely to disclose their information than those who are not endowed with either privacy or service (the choice condition).*

H1b: *Those who are endowed with a service are more likely to disclose their information than those who are not endowed with either privacy or service (the choice condition).*

6.1.2 Disclosure Nudge, a Heuristic Manipulation

Platform designers sometimes nudge users of digital products towards selecting a specific option [48, 150, 179, 22, 146]. Please see chapter 3, subsection 3.1.2 and chapter 5, subsection 5.2.3 for a detailed discussion about nudges. In this study, the nudge that I use highlights the desired option and plays down the undesired choice. Figure 6.2 shows a nudge where the desired option is highlighted in green, and the undesired option is played down using a fade gray color. This nudge is an example of dark pattern design, where platform designers want to maximize data disclosure [211, 210, 233]. Scholars used this type of nudge in previous studies and found that this nudge promotes disclosure behavior [306, 203, 233]. In line with these findings, I pose the following hypothesis:

H2: *Users are more likely to disclose data in the presence of disclosure nudges.*

6.1.3 Strategic Disclosure, a Calculated Decision

Privacy calculus framework suggests that users of digital products make a trade-off between the risks and the benefits of disclosure prior to making the disclosure decision [185, 67, 84]. It follows that if the users believe disclosing data will improve their user experience or can lead to benefits, they will have higher disclosure intentions [332]. On the contrary, behavioral intentions to disclose data will be lower if the disclosure is associated with increased perceived privacy risks [332] (see chapter 2 for a thorough discussion about privacy calculus). Furthermore, Xu et al. [332] measured the outcome of the risk and benefit trade-off in the perceived value of information disclosure such that a high risk perception will decrease the overall perceived value of disclosure while a higher benefit perception will increase the overall perceived value of disclosure.

In line with the privacy calculus, I hypothesize that if a data type has the potential to benefit users, they perceive disclosure as more beneficial and less risky. In addition, perceived value mediates the effects of perceived risk and benefit on disclosure:

H3a: *Users find disclosure of a data type that can improve their user experience as more beneficial.*

H3b: *Users find disclosure of a data type that can improve their user experience as less risky.*

H4a: *If users perceive a disclosure as being beneficial, they are more likely to consider disclosure more valuable.*

H4b: *If users perceive a disclosure as being risky, they are less likely to consider disclosure less valuable.*

H5: *The perceived value positively predicts disclosure behavior.*

6.1.4 Digital Literacy and Privacy Self-efficacy

Privacy research shows that users with high digital literacy are more likely to manage their privacy compared to those with low digital literacy [241]. In the context of social media, for example, those with higher levels of digital privacy literacy show more privacy control behaviors and feel safer on the online platforms [39]. On the other hand, a lack of digital literacy prevents users from using the technology to its full potential and makes them susceptible to online threats [320, 268]. For instance, users with low levels of awareness concerning protective privacy strategies are less likely to opt-out from a telephone directory listing[97].

These findings can be justified through the ELM. Digital privacy literacy is an individual's ability to make an elaborated decision. Users of digital products who have high privacy literacy can better control their information and align their disclosure behaviors with their attitudes as they are better equipped with the knowledge to do so. Thus, for individuals with high (vs. low) digital literacy, the effect of heuristic aspects of decision is weaker, while the impact of cognitively moderated elements of the decision is more substantial:

H6a: *The effects of endowment heuristics on disclosure behavior is weaker for users with high digital privacy literacy.*

H6b: *The effects of disclosure nudges on disclosure behavior is weaker for users with high digital privacy literacy.*

H7: *The effects of perceived value on disclosure behavior is stronger for users with high digital privacy literacy.*

Similar to digital literacy, privacy self-efficacy is related to one's control over their behaviors [14]. However, digital literacy is one's ability to perform digital tasks, while self-efficacy relates to the beliefs one has about their ability to conduct specific tasks [34]. Individuals with high self-efficacy show more confidence in achieving their goal [34], and are able to perform digital tasks easier [10]. Having a higher privacy self-efficacy is associated with showing more privacy-protective behaviors [184]. In the context of social media, for example, users with high privacy self-efficacy engage in protective privacy behaviors such as limiting their profile visibility [73].

The ELM can also justify the effects of self-efficacy on disclosure decisions. Previous work conceptualizes privacy self-efficacy as the ability to make privacy decisions [172]. Those who believe they lack the ability to manage their privacy (i.e., suffering from a low privacy self-efficacy) are less likely to invest cognitive effort in their decisions and more likely to use decision shortcuts. On the contrary, those who believe that they have the ability to manage their privacy are more likely to invest some cognitive effort into their privacy decision and less likely to use decision shortcuts. For these individuals, the effects of heuristic aspects of the decision is weaker, while the impact of cognitively moderated aspects of the decision is more substantial:

H8a: *The effects of endowment heuristics on disclosure behavior is weaker for users with high privacy self-efficacy.*

H8b: *The effects of disclosure nudges on disclosure behavior is weaker for users with high privacy self-efficacy.*

H9: *The effects of perceived value on disclosure behavior is stronger for users with high privacy self-efficacy.*

6.1.5 Privacy Concerns as a Motivation to Elaborate

Individuals who have high privacy concerns have a higher motivation to manage their privacy [51, 25]. The main body of privacy literature is concerned with the direct behavioral effects of privacy concerns on disclosure intentions and behaviors. The common finding in these studies is that highly concerned individuals are less likely to disclose information [94, 15, 337, 139, 122]. While many studies investigated the main effect of privacy concerns on behavior, few studies explored the moderation effects of privacy concerns. Tan et al. [293] found that privacy concerns moderate the relationship between users' attitudes and behaviors such that highly concerned users are more likely to use social networking websites only if they find it beneficial.

We can study the effects of privacy concerns on disclosure decisions through the lens of ELM. Previous studies conceptualized privacy concerns as motivations for individuals to engage in issue-relevant thinking and elaborate the decision scenario [25, 37, 172]. For example, Bansal et al. [37] studied how privacy concerns influence users' perceived trust in a website and, in turn, their intention to disclose information to that website. They found that peripheral cues such as website design and reputation are less important for highly concerned individuals (who use the central route) and more important for users with low levels of privacy concern (who use the peripheral route). On the other hand, the website's privacy policy is more important for individuals with great concerns and less important for individuals with fewer concerns. Overall, these findings suggest that highly privacy-concerned individuals are motivated to elaborate the decision scenario (i.e., use the central route). On the contrary, those with lower levels of concern are not as motivated to take charge of their privacy and will invest a lower cognitive effort in their privacy decisions (i.e., use the peripheral route). In line with these findings, I pose the following hypotheses:

H10a: *The effects of endowment heuristics on disclosure behavior is weaker for users with high privacy concerns.*

H10b: *The effects of disclosure nudges on disclosure behavior is weaker for users with high privacy concerns.*

H11: *The effects of perceived value on disclosure behavior is stronger for users with high privacy concerns.*

H12: *Users with high privacy concerns are less likely to disclose information.*

6.1.6 The Relationship Between Age and Privacy Literacy, Self-efficacy, and Concerns

While scholars in different fields predominantly assume that older adults have comparatively lower levels of digital literacy [47, 310, 301, 16, 107, 272], the empirical findings in the privacy literature do not support such an assumption. Kezer et al. [163] for example, studied privacy literacy among young, middle-aged, and older adult Facebook users and did not find any significant differences across these groups. The literature even includes results contradictory to the mainstream assumption; Hoofnagle et al. [134] asked several privacy questions from young and older adult age groups. They found that older adults did better in answering the questions than younger adults. Although the empirical studies do not show a consistent relationship between age and privacy literacy, I pose a hypothesis in line with the mainstream literature:

H13: *Older adults have lower levels of privacy literacy compared to young adults.*

However, the narratives in the literature and the empirical findings regarding the relationship between age, self-efficacy, and privacy concerns are consistent. Literature mentions older adults' lack of self-efficacy and high privacy concerns as barriers towards their interactions with technology [321, 301, 250, 107]. Many empirical findings support the general trend that older individuals have higher concerns and lower self-efficacy [133, 117, 340, 307]. However, most of these sources study age as a linear variable and show a general trend. For example, Hoffmann et al. [133] studied 1,488 Internet users and found that age is negatively related to self-efficacy but positively associated with privacy concerns. I further contribute to the literature by specifically focusing on older and younger adults. In line with the literature, I pose the following hypotheses:

H14: *Older adults have lower levels of privacy self-efficacy compared to young adults.*

H15: *Older adults have higher levels of privacy concerns compared to young adults.*

6.2 Methods

I developed a browser-based recommender application, "RecipeDigger," to study the hypothesized effects. The application claimed to provide a diverse set of food recipes and be linked to a rich database of international food recipes. To maximize ecological validity, I registered the app on a valid domain, 'recipe-digger.com.' While the application was realistic-looking, it was fictations and could not deliver any food recipe recommendations. This information was withheld from the

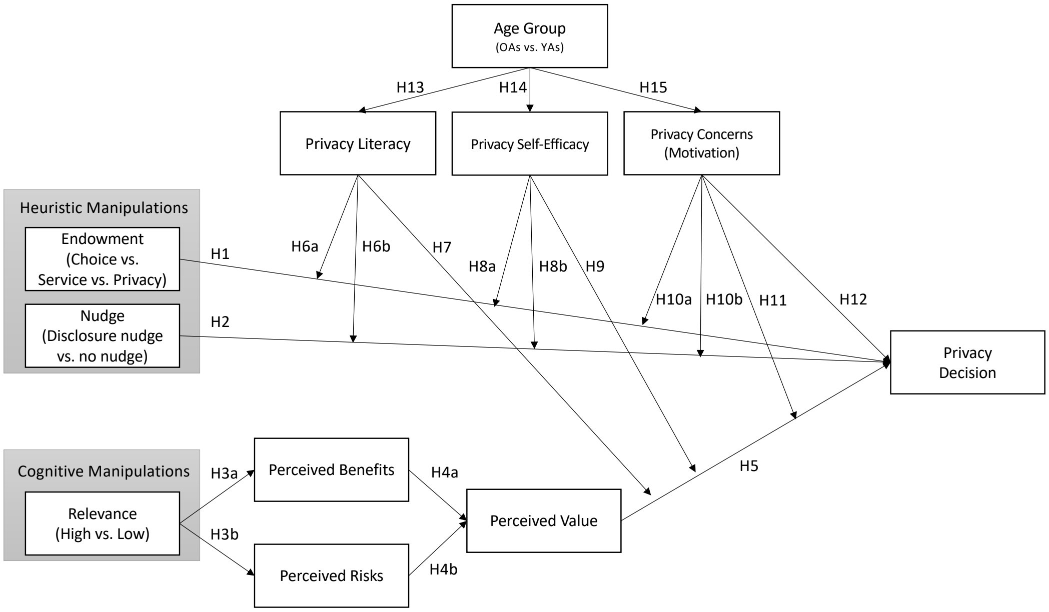
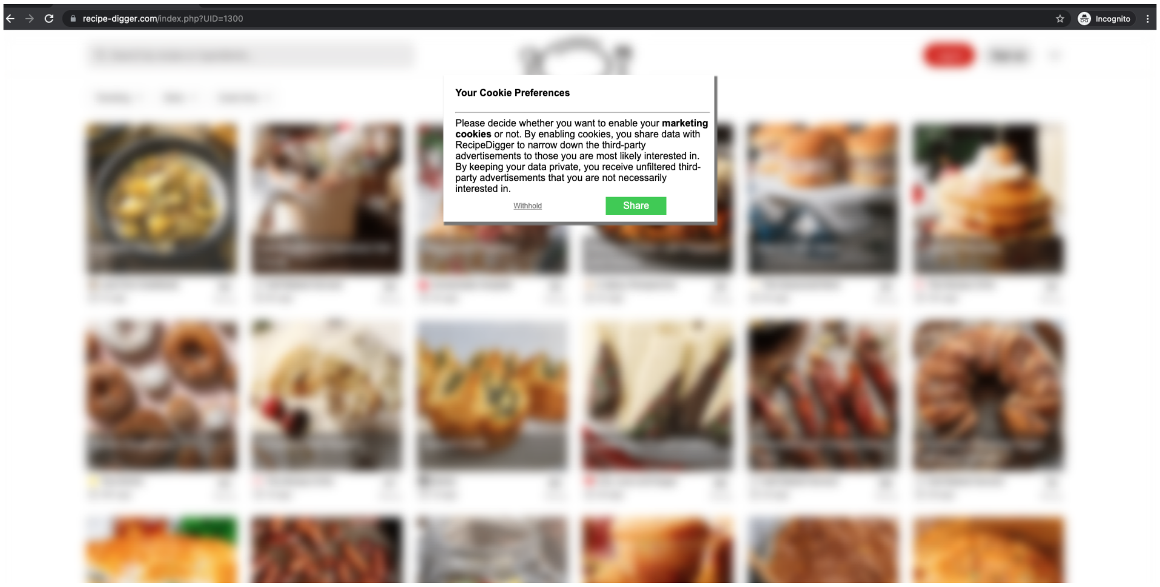


Figure 6.1: An overview of the hypothesized model.

Participants until the end of the study. Figure 6.2 shows the RecipeDigger application.

I added a personalization feature to the application to make it a suitable scenario for studying privacy decision-making. Personalization is a popular scenario in privacy research [27, 13, 331, 289]. In a personalization scenario, users give up their privacy to receive a personalized service. This allows scholars to investigate individuals' disclosure behaviors with respect to their perceived benefits resulting from disclosure. In the RecipeDigger application, participants could enable the app to set cookies for personalization purposes.

A cookie consent notice is required by Europe's General Data Protection Regulation (GDPR) before setting cookies and collecting user data [87]. To meet this requirement and still collect as much data as possible, companies use maximize dark pattern designs [233] (see chapter 5 for a thorough discussion about maximize dark patterns). The wide usage of cookie consent notices encouraged privacy scholars to study them and identify their treats to users' online privacy [306, 203, 233]. For example, Ultz et al.[306] showed that nudging users by highlighting disclosure option increases compliance rates. I also operationalize this study using a cookie consent scenario to contribute to this body of literature.



Your Cookie Preferences

Please decide whether you want to enable your **marketing cookies** or not. By enabling cookies, you share data with RecipeDigger to narrow down the third-party advertisements to those you are most likely interested in. By keeping your data private, you receive unfiltered third-party advertisements that you are not necessarily interested in.

Figure 6.2: An overview of the recipe-digger.com website

6.2.1 Procedure

In the recruitment script, participants were told that we were developing a food recipe application, and their task is to interact with the application and answer some questions about their interaction. Participants who were willing to participate in the study read and agreed to the consent form. Then, they were redirected to the application, where I measured the dependent variable.

6.2.2 Dependent Variable: Accepting/Rejecting Cookies

After participants were redirected to the RecipeDigger, they could view the website for one second. Then, a pop-up notice about cookies appeared and blurred the website view. Participants had to respond to this pop-up window to proceed with the study. The pop-up window asked them whether they agreed to share data with the website through cookies or not. Participants could agree with data sharing and click the ”share” button or reject the data sharing by clicking the ”withhold” button. The disclosure decision is the main dependent variable in this study.

6.2.3 Experimental Manipulations

In this section, I present the independent variables that I implemented in the form of experimental manipulations. All of the experimental manipulations are presented as between-subject.

6.2.3.1 Endowment Condition

In order to study the effects of endowment heuristic on user decisions, I presented the cookie notice with either of the three versions of privacy endowed, service endowed, or choice. The privacy endowed version attempts to endow users with their privacy and present data disclosure in return for obtaining a service as an alternative. The service endowed version endows users with the service and presents withholding data (i.e., privacy) and not having the service as an alternative. Finally, the choice option is a neutral condition where users are not endowed, and both privacy and service are offered as options. The wordings of the three endowment conditions are presented below:

- Privacy endowed: Your data is currently **kept private** from RecipeDigger; (**functional cookies/marketing cookies**) are disabled, which means that you will receiving unfiltered (recipe recommendations/third-party advertisements) that you are not necessarily interested in. However, you can use the enable button to share your data and receive (recipe recommendations/ third-party advertisements) that are narrowed down to the ones that you are most likely interested in.

- Service endowed: Your data is currently **shared** with RecipeDigger; (**functional cookies/ marketing cookies**) are enabled, which means that you will receive (recipe recommendations/ third-party advertisements) that are narrowed down to the ones that you are most likely interested in. However, you can use the disable button to make your data private and receive unfiltered (recipe recommendations/third-party advertisements) that you are not necessarily interested in.

- Choice: Please decide whether you want to enable or disable your (**functional cookies/ marketing cookies**). By clicking the enable button, you share data with RecipeDigger, which means that you will receive (recipe recommendations/third-party advertisements) that are narrowed down to the ones that you are most likely interested in. By clicking the disable button, you make your data private from RecipeDigger, which means that you will receive unfiltered (recipe recommendations/ third-party advertisements) that you are not necessarily interested in.

As Figure 6.2 shows, participants were able to click on either the ”share” or the ”withhold” buttons. In the privacy and service endowed conditions, users could also ’close’ the cookie popup by clicking the 'X' button at the top right corner of the dialogue box. Clicking the 'X' button means that users are willing to proceed without changing anything (i.e., they share information in service endowed and withhold in privacy endowed). However, the choice condition did not have the 'X' button as users are not endowed with anything and must select an option.

6.2.3.2 Disclosure Nudge

A critical aspect of a nudge is that it highlights the desired option and plays down the undesired choice [48]. A common method for highlighting the favorable option is depicting it in green color [2]. This leads to users perceiving the green option as favorable. While the desired options are highlighted, the undesired options are played down (e.g., by being presented in smaller font and bland colors [48, 2]). To operationalize disclosure nudges, I highlighted options giving consent to disclosure in green and presented the options refraining from disclosure with a smaller font and a fade color. For the no nudge condition, I presented "share" and "withhold" buttons consistently in gray boxes and with similar font sizes.

6.2.3.3 Cookie Type

To manipulate the cognitive aspects of the decision, the application asked for either "functional cookies" or "marketing cookies." Functional cookies can benefit users by facilitating the functionality of a website and boosting the user experience [276]. Marketing cookies, however, collect information for third-party companies and are only used for targeted advertisements [276]. Users perceive targeted advertisements as privacy-intrusive services [106, 101]. Therefore, while setting functional cookies can benefit users, setting marketing cookies does not serve the goal of a given website, and individuals are less likely to be in favor of marketing cookies [212, 276, 251]. Deciding whether accepting functional and marking cookies are advantageous is a cognitive task that requires individuals to think about the goal of the application.

6.2.4 Survey Measures

After participants interacted with the application, they were redirected to a survey. The instructions in the survey told them that they should answer some questions before they could proceed with the application. At the end of the study, they were debriefed that the application was not real and did not set any cookies. As the study involved deception, participants had a chance to discard their data without compromising their incentives.

6.2.4.1 Perceived Risks and Benefits

Perceived risks and benefits of the disclosure are two important variables relating to the privacy calculus framework. To measure these variables, I asked participants' perceptions on the level of benefits (accepting functional/marketing cookies can improve the quality of the recipes I receive) and risks (accepting functional/marketing cookies is risky) of accepting cookies on a 7-point agreeableness Likert scale.

6.2.4.2 Privacy Literacy, Self-efficacy, and Concerns

To measure privacy literacy, I used the Online Privacy Literacy Scale (OPLIS) [207]. This scale measures individuals' knowledge about concepts relating to privacy (e.g., if they know what a 'cookie' is) by having them answering to several multiple choice questions. Participants will be scored based on their correct answers. Please check Appendix A to see the questions. In addition, I adopted Kobsa et al.'s .[172] privacy self-efficacy and Malhotra et al.'s [205] data collection concerns scales. Table 6.1 in the results section shows these instruments.

6.2.4.3 Data Analyses

I used Anova and regression analyses to study H1-H4, H11, and H12-H14. To study the moderation effects (H5-H10), I conducted several models with random slopes to allow variations in moderation effects(slopes). I will run these models such that we understand the moderating effects of the three moderating variables (i.e., digital literacy, privacy self-efficacy, and privacy concerns), the mediated moderating effects of age through these variables, and the unmediated moderating effects of age. All the analyses were carried out in Mplus v7.

6.3 Results

6.3.1 Descriptive Statistics

625 participants, including 381 younger adults (184 males, 176 females, 3 transgenders, 14 non-binary, and 4 who preferred not to disclose their gender) and 244 older adults (95 males, 149

females), were recruited through the Prolific recruiting platform. The average age of younger adults was 21.9 ranging from 18 to 25 years old (SD = 2.37). The age of older adult participants ranged from 55 to 88 with an average of 69.7 (SD = 4.38).

6.3.2 Construct Reliability

To measure privacy literacy, I calculated the number of correctly-answered questions on the OPLIS scale for each participants [207]. This scale includes 7 questions. Therefore, participants' privacy literacy scores varies from 0 to 7 (median = 4.92, SD = 1.56).

In addition to OPLIS, I borrowed several other measurement instruments from the literature. Although these instruments were already validated in the previous studies, I calculated Cronbach's alpha as a measure of internal consistency [54]. All of the constructs have an alpha above the acceptable threshold of 0.7 [234] (see Table 6.1). In addition, I studied the reliability of the constructs using Confirmatory Factor Analysis (CFA). Besides a removed item from perceived value, all the items shown in Table 6.1 have a high loading (mostly above 0.7), suggesting convergent validity. The CFA model has an acceptable fit; although the chi-squared is slightly high ($\chi^2(109) = 435.608$, $p < 0.001$) and RMSEA is slightly above the accepted cutoff of 0.05 (RMSEA = 0.069), CFI and TLI are 0.989 and 0.986, suggesting an acceptable fit [114]. In addition, Table 6.2 reports the correlations and the Average Variances Extracted (AVE, the main diagonal). All the correlations are below the AVE for all constructs, suggesting discriminant validity. Therefore, I use the factor scores of the constructs in my analyses.

6.3.3 Testing the Hypotheses

Below, I first study the main effects. Then, I report the mediated and unmediated moderation effects.

6.3.3.1 Main Effects

While being endowed by privacy (vs. choice) decreases the odds of accepting the cookie notice, this effect does not reach significance thresholds ($p = 0.363$—H1a rejected). However, compared to the choice condition, those endowed by service are 1.29 times more likely to accept the cookie notice (OR = 1.29, $p = 0.023$—H1b supported). Likewise, those who see a disclosure nudge are 1.11

Subjective Construct	Items	Factor loadings
Privacy Self-efficacy alpha: .822 AVE: .810	I know how to identify sites with secure servers	0.709
	I know how to evaluate online privacy policies.	0.825
	I know how to change the security settings of my browser to increase privacy.	0.823
	I know how to use a virus scanning program.	0.788
	I know how to block unwanted E-mails.	0.650
Collection Concerns alpha: .897 AVE: .892	t usually bothers me when online companies ask me for personal information.	0.885
	When online companies ask me for personal information, I sometimes think twice before providing it.	0.787
	It bothers me to give personal information to so many online companies.	0.950
	I'm concerned that online companies are collecting too much personal information about me.	0.864
Perceived Risks alpha: .901 AVE: .907	Providing RecipeDigger with Functional/Marketing cookies would involve many unexpected problems.	0.889
	It would be risky to disclose data to RecipeDigger by enabling Functional/Marketing cookies.	0.879
	There would be a high potential for loss in disclosing data to RecipeDigger by enabling Functional/Marketing cookies.	0.903
Perceived Benefits alpha: .928 AVE: .918	Providing RecipeDigger with Functional/Marketing cookies can reduce the time I need for finding what I want on RecipeDigger.	0.892
	Interacting with RecipeDigger will be more convenient if I enable the Functional/Marketing cookies.	0.950
	Overall, I feel that enabling Functional/Marketing cookies facilitates my interactions with RecipeDigger.	0.926
Perceived Value alpha: .805 AVE: .965	I think the benefits I would gain from enabling Functional/Marketing cookies can offset the risks of my information disclosure.	0.919
	The value I gain from enabling Functional/Marketing cookies is worth the information I give away.	0.944
	I think the risks of my information disclosure will be greater than the benefits gained from enabling Functional/Marketing cookies.	-0.588

Table 6.1: The results of the Confirmatory Factor Analyses

Constructs	Collection Concerns	Privacy Self Efficacy	Perceived Risks	Perceived Benefits	Perceived Value
Collection Concerns	0.892				
Privacy Self Efficacy	0.268	0.810			
Perceived Risks	0.437	-0.044	0.907		
Perceived Benefits	-0.129	0.231	-0.275	0.918	
Perceived Value	-0.408	0.087	-0.579	0.721	0.965

Table 6.2: The correlation matrix. The diagonal values represent AVE

times more likely to accept the cookie notice than those who do not see a disclosure nudge (OR = 1.11, p=0.017—H2 supported).

Furthermore, participants find accepting a functional cookie notice as more beneficial, such that a cookie notice requesting to set functional cookies (vs. marketing cookies) results in higher levels of perceived benefits by 0.299 standard deviation (β = 0.299 ,p<0.001—H3a supported). In addition, setting a functional cookie is perceived as less risky; participants perceive -0.119 standard deviation less risks by setting such cookies (β = -0.119, p=0.002—H3b supported). Likewise, by one standard deviation increase in perceived benefits the perceived value of accepting the cookie notice increases by 0.762 times standard deviation (β = 0.762, p<0.001—H4a supported). In addition, by one standard deviation increase in perceived risks, the perceived value of accepting the cookie notice decreases by 0.628 times standard deviation (β = -0.628, p<0.001—H4b supported). Furthermore, the results show that the perceived value of disclosure is a strong predictor of accepting the cookie notice such that by one standard deviation increase in perceived value, individuals are 4.22 times more likely to accept the cookie notice (OR = 4.22, p<0.001—H5 supported). Lastly, one standard deviation increase in privacy concerns would decrease the odds of accepting the cookie notice by 0.29 times (OR = 0.29, p<0.001—H12 supported).

In addition to the main effects, I explored the effects concerning age; the mediated and unmediated moderation effects of age by privacy literacy, privacy self-efficacy, and privacy concerns regarding these main effects. When the effect of a variable on privacy decision is moderated by either privacy literacy, privacy self-efficacy, or privacy concerns, we have mediated moderation. When neither of these three variables moderated the effect of a variable on privacy decision, but age does, we have an unmediated moderation.

6.3.3.2 Age and Its Mediated Moderation Effects

The data suggests that older adults have higher privacy literacy (β = 0.196, p=0.001–H13 rejected), higher privacy self-efficacy (β = 0.149, p=0.001–H14 rejected), and higher privacy concerns (β = 0.205, p = 0.001–H15 supported). Below, I report whether these three variables mediate the moderation effects of age or not.

Privacy Literacy: The results do not show any mediated moderation effects concerning the heuristic manipulations: the effects of endowment or nudge on cookie acceptance decision are not moderated by privacy literacy (ps > 0.05—H6a and H6b rejected). Regarding the mediated moderation of the cognitive effect—perceived value of disclosure—privacy literacy moderates the effects of perceived value on cookie acceptance decision (β = 0.604, p=0.001—H7 supported). This means that the effects of perceived value on accepting cookie notices is stronger for those with higher privacy literacy (see figure Figure 6.3).

Privacy Self-efficacy: The results do not show any mediated moderation effects concerning the heuristic manipulations: the effects of endowment or nudge on privacy decision is not moderated by privacy self-efficacy ($ps > 0.05$—H8a and H8b rejected). With regards to the cognitive effect, privacy self-efficacy does not moderate the effect of perceived value on cookie acceptance decisions (β = 0.348, p=0.104—H9 rejected).

Privacy Concerns: The results do not show any mediated moderation effects concerning the heuristic manipulations: the effects of endowment or nudge on privacy decision are not moderated by privacy concerns ($ps > 0.05$—H10a and H10b rejected). Likewise, privacy concerns do not moderate the cognitive aspect—the effect of perceived value—on cookie acceptance decision-0.262 (β = -0.224, p=0.263—H11 rejected).

6.3.3.3 Unmediated Moderation Effects

Overall, I found two unmediated moderation effects. Firstly, the effect of endowment on cookie acceptance decision is moderated by age ($\chi^2(1) = 6.463, p = 0.011$) such that the overall effect of being endowed by service on accepting the cookie notice is weaker for older adults (β = -1.278, p=0.006). However, the effect of endowment by privacy on cookie acceptance decision is not different per age groups (β = 0.104, p>0.05). Figure 6.4 shows this effect.

I studied the previous findings in isolation of other effects. In the next section, I report my analyses concerning the full path model.

6.3.4 Full Path Model

I conducted a full path model; in addition to all the hypothesized effects (see Figure 6.1), I regressed heuristic manipulations on perceived risks, benefits, and value and included the possible moderation effects by the three moderator variables as well as the age group. Furthermore, I considered the three moderators and the age group as potential moderators of the effect of perceived risks and benefits on perceived value. Lastly, I studied any potential direct effects of perceived risks and benefits on the cookie acceptance decision and whether any of the three moderators or age

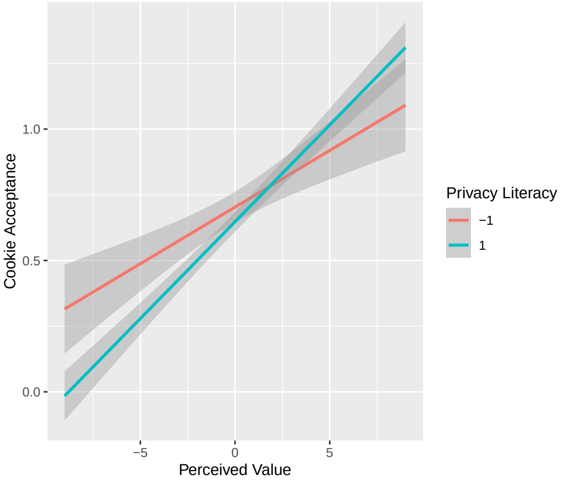


Figure 6.3: Privacy literacy mediates the effect of perceived value on cookie acceptance decision.

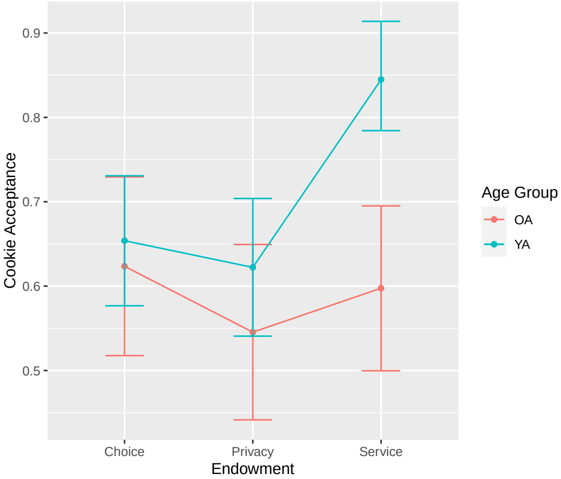


Figure 6.4: While younger adults endowed by service disclose data, older adults are not being influenced by the endowment.

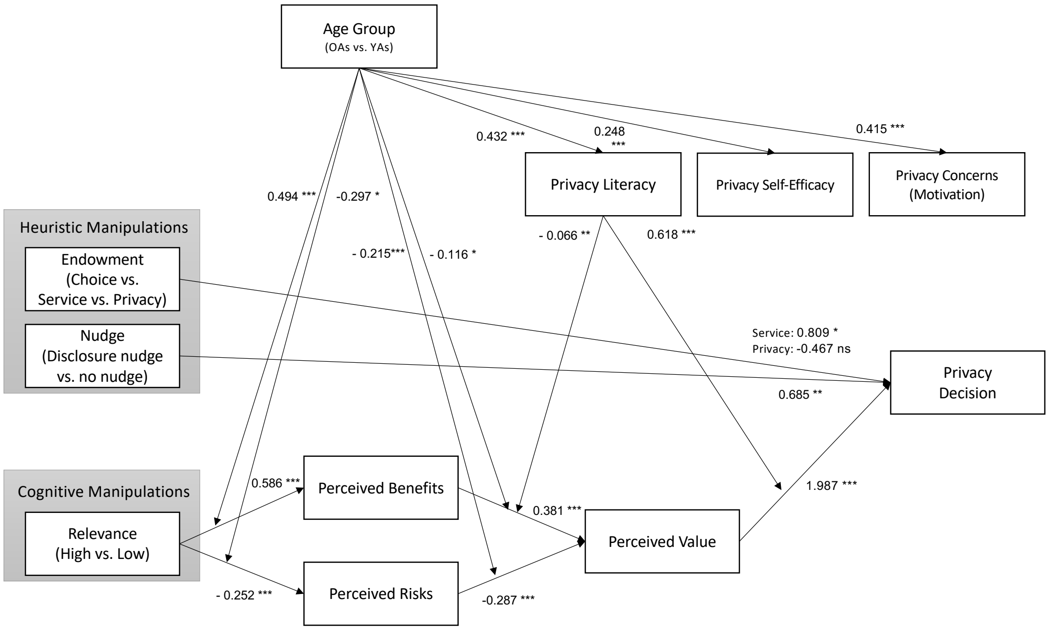


Figure 6.5: The results of full model. To keep the figure readable, I did not show the non-hypothesized main effects. Please refer to Table 6.3 for the full results.

moderates these effects. Then, I then trimmed the non-significant effects. This led to several new effects.

Firstly, I found several unmediated moderation effects of age. The effects of perceived risks and benefits on perceived value were moderated by age; by one standard deviation increase in perceived risks, older adults perceive 0.215 times standard deviation less value than younger adults ($p < 0.001$). In addition, by one standard deviation increase in perceived benefits, older adults perceive 0.116 times standard deviation less value than younger adults (p=0.048). Furthermore, the effect of relevance on perceived risks and benefits was stronger for older adults; when asked about setting a relevant cookie (i.e., functional cookie), they perceived less risks (β = -0.297, p=0.022) and more benefits (β = 0.494, p<0.001) than younger adults.

Secondly, I found an additional mediated moderation effects of age; the effects of perceived risks on perceived value were stronger for those with higher privacy literacy (β = -0.066, p=0.008). Table 6.3 reports the final results. I also present these results in Figure 6.5.

Variable	Beta (OR for Privacy Decision)	Standard Error	P-value
DV: Privacy Decision			
Privacy Literacy	-0.039 (0.96)	0.113	0.728
Age Group (OA vs. YA)	-0.254 (0.77)	0.385	0.492
Nudge	0.685 (1.98)	0.231	0.002
Endowment			
-Privacy (vs. Choice)	-0.467 (0.62)	0.272	0.085
-Service (vs. Choice)	0.809 (2.24)	0.314	0.010
Endowment X Age Group	$\chi^2(1) = 2.579$	-	0.108
-Privacy X OA	-0.391 (0.67)	0.552	0.478
-Service X OA	-1.306 (0.27)	0.643	0.032
Perceived Value	1.987 (7.29)	0.326	<0.001
Perceived Value X Privacy Literacy	0.618 (1.85)	0.167	<0.001
DV: Perceived Value			
Privacy Literacy	-0.048	0.022	0.031
Privacy Concerns	-0.151	0.029	<0.001
Age Group (OA vs. YA)	0.100	0.044	0.021
Perceived Risks	-0.287	0.034	<0.001
Perceived Benefits	0.381	0.031	<0.001
Perceived Risks X Age Group	-0.215	0.061	<0.001
Perceived Risks X Privacy Literacy	-0.066	0.025	0.008
Perceived Benefits X Age Group	-0.116	0.059	0.048
DV: Perceived Risks			
Privacy Literacy	-0.081	0.039	0.021
Privacy Concerns	0.532	0.036	<0.001
Privacy Self-efficacy	-0.157	0.040	<0.001
Age Group (OA vs. YA)	0.035	0.075	0.261
Relevance (Relevant vs. Non-relevant)	-0.252	0.065	<0.001
Relevance X Age Group	-0.297	0.130	0.022
DV: Perceived Benefits			
Privacy Concerns	-0.289	0.041	<0.001
Privacy Self-efficacy	0.196	0.042	<0.001
Age Group (OA vs. YA)	-0.014	0.075	0.856
Relevance (Relevant vs. Non-relevant)	0.586	0.070	<0.001
Relevance X Age Group	0.494	0.142	<0.001
DV: Privacy Concerns			
Age Group (OA vs. YA)	0.415	0.075	<0.001
DV: Privacy Literacy			
Age Group (OA vs. YA)	0.432	0.077	<0.001
DV: Privacy Self-efficacy			
Age Group (OA vs. YA)	0.248	0.074	<0.001

Table 6.3: The trimmed path model

6.4 Discussion

To study the mediated moderating effects of age, I designed an online experiment where individuals make a privacy decision to accept or reject cookie notices. I applied experimental manipulations motivated by both cognitive and heuristic aspects of the disclosure decision. My findings contribute to the field in several ways.

Firstly, the finding can inform the legislative bodies and policy developers regarding the cookie consent notices. Despite the regulations on allowing users to make informed privacy decisions, online platforms use dark pattern designs where they manipulate cookie notices in several ways to maximize data disclosure [233]. My results show that these manipulations (i.e., dark design patterns) are effective and can influence users' free choice. For example, I showed that a disclosure nudge or endowing users with a service could promote data disclosure by accepting cookie notices. In addition, my results show that education may not be a way to promote an informed decision in the presence of such heuristic dark patterns as privacy literacy nor privacy self-efficacy do not moderate the disclosure maximizing effects of such dark designs. It is necessary for supplementary regulations to further restrict using dark pattern designs and standardize cookie notices.

This study points towards education not as a way to confront dark pattern designs, but as a way to promote an informed choice—the cognitive aspect of privacy decisions. Users with heightened privacy literacy can align their disclosure decisions with their preferences (perceived value) better. Therefore, while the legislative bodies such as the European Union must require companies to follow transparent procedures for obtaining informed consent (to address the heuristic aspect), they should also invest in educational programs to enhance digital literacy among the population.

In addition, while most studies in this dissertation and in the literature focus on either cognitive or heuristic aspects of privacy decisions, I designed experimental manipulations that target both of these aspects. I designed endowment and disclosure nudge manipulations that are thought to *subconsciously* influence individuals' decisions. Indeed, nudge and endowment did not significantly influence privacy calculus (i.e., the perceived risks, benefits, and value of disclosure—($ps > 0.05$). Therefore, we can conclude that these manipulations operate in a subconscious level. In addition, I introduced the data relevance (functional vs. marketing cookies) as an experimental manipulation that was thought to manipulation the decision via a *conscious* process (e.g., privacy calculus). Consequently, relevance significantly influenced privacy calculus (see Table 6.3). This is an important contribution as I show that privacy decisions are neither heuristic nor fully rational [56, 5]. I urge future studies to employ a dual-route approach and study their outcome variable of interest from both a heuristic and rational perspectives.

Furthermore, this study makes several contributions to the older adults and technology use literature. My results rebut the deficit-based narrative suggesting that older adults do not have sufficient knowledge about technology and cannot manage their technology interactions. I used the ELM framework to explore this deficit-based narrative from two perspectives: older adults' *ability (i.e., privacy literacy and self-efficacy)* and their *motivation (i.e., privacy concerns)* to control their technology interactions. My results showed that older adults, indeed, have the ability (i.e., higher privacy literacy and privacy self-efficacy) compared to younger adults. They are also more motivated to control their privacy as they had greater privacy concerns. However, this is noteworthy that all of the participants in this study were recruited via Prolific, a crowd-sourcing platform. Older adults are arguably not a monolith population and have different levels of digital literacy. Older adults who participated in this study may be a sub-set of the older adult population who, overall, have higher levels of digital literacy.

The results also show that older adults are more likely to process their decisions cognitively and less likely to use decision heuristics than younger adults. This is in line with previous findings [20]. At the basic stage of privacy calculus, assessing the risks and benefits of disclosure, older adults are more attentive to the cognitive cues (i.e., perceived relevance); if they find a disclosure relevant, they will consider disclosure of that data as less risky and more beneficial. Furthermore, perceived risks is a stronger predictor of perceived value for older adults. This is also in line with previous literature suggesting that older adults are more loss-averse than younger adults [60]. In addition to relying more on cognitive aspects of the decision, older adults also rely less on the heuristic aspects. While being endowed by service increases disclosure for younger adults, older adults are not being influenced by the endowment effect (see Figure 6.4).

The selection, optimization, and compensation model can justify these findings. As older adults' cognitive and physical resources decline, they adopt their goals from a growth focus to a maintenance or a loss-prevention focus [31, 64]. This makes older adults more selective in effort allocation; they tend to optimize their performance by investing more effort in tasks that have a higher value to them [129]. Older adults who participated in this study were highly motivated to be engaged with the task as they were highly concerned about losing their privacy. Therefore, they chose to invest effort in this cookie acceptance decision scenario. Consequently, when they made their privacy decision, they allocated more cognitive effort and used the central route (i.e., privacy calculus) more than the peripheral route (i.e., decision heuristics).

However, I found that this difference can be traced to the different levels of privacy literacy among the two populations, as these variables mediate the moderating effects of the age group. Overall, individuals with a high privacy literacy are more likely to take control of their privacy as the effects of the cognitive aspect of the decision (perceived value) on privacy decision is stronger for them. On the contrary, these effects are reversed for those with low levels of privacy literacy, such that individuals with lower literacy are not as able to align their disclosure decision with their perceived value of disclosure. Furthermore, the process of privacy calculus is more robust for individuals with higher literacy; having higher literacy helps individuals identify risks better and adjust their perceived values. The moderating effects that I studied were not unique to older adults and applied to younger adults as well. This shows that being an older adult in and of itself does not influence disclosure decisions. Instead, a major part of the difference between older and younger adults in the decision process is a function of different levels of privacy literacy.

This study extends the theories in psychological ownership [156, 8] by showing that the concept of endowment not only applies to tangible physical goods but also applies to digital products. I was the first who studied the endowment within the context of privacy and through an online experiment. Endowing individuals with a service will increase the odds of them wanting to maintain the service and being willing to disclose their data in return.

Furthermore, these findings contribute to privacy literature by showing the parameters that increase the elaboration likelihood of privacy decisions. Elaboration is more likely for the individuals who possess the ability (digital privacy literacy).Within an ELM lens, such persons process the information by the central route and spend cognitive effort on the decision. However, persons who lack such abilities process the information through the peripheral route.

6.5 Limitations and Future Work

The older adults who participated in this study may not be a representative sample of older adults. I recruited older adult participants from an online crowd-sourcing platform. Therefore, all older adults in this study have experiences with computers and are relatively tech-savvy. Future studies should also study older adults who do not interact with computers as much. In addition, my sample is limited to US-based individuals. Future research should study older adults from different countries with different cultures for two reasons. Research suggests that individuals from different countries have diffident perceptions about privacy [195, 194], and different thinking processes [114].

Furthermore, I used a recipe provider application as the experimental scenario. Cooking food and looking for new recipes may be interesting to some individuals while some others may not even cook at their home. While I controlled for this potential confound with perceived benefits and perceived values of disclosure, future studies should use a more neutral scenario where individuals have similar attitudes in favor of that topic.

In addition, this study showed that younger adults have lower levels of digital privacy literacy and privacy self-efficacy. However, it did not seek out ways to improve this situation. Future research should focus on ways to educate technology users and enhance their levels of privacy literacy.

6.6 Conclusion

I studied the impact of privacy literacy, self-efficacy, and concerns on older and younger adults' privacy decisions. My results show that while older adults' decision process is different than younger adults, this difference can be attributed to the differences in the levels of privacy literacy between older and younger adults. The results showed that one of the main difference in thinking mechanisms of older vs. younger adults springs from this variable.

Chapter 7

General Conclusion and the Future Directions

7.1 Empowering Older Adults With Their Privacy

This document rebuttals the view that depicts older adults as individuals inattentive to their privacy and shows directions towards empowering the older population to use technology products. In chapter 4, I found that older and younger adults have different privacy decision-making mechanisms; older adults are willing to invest more effort into the decision scenario and are more likely to disclose data if they find it beneficial. These findings support the growing body of literature that adopts a strength-based view rather than the deficit-based view and can better lead to older-adults-friendly technologies [109, 177, 20].

Since older adults are *attentive* to their privacy, platform designers should avoid design strategies that are not older adult-friendly. For example, chapter 5 shows that dark pattern designs disproportionately influence older adults and put older adults at a disadvantage: older adults are more likely to fall prey to framing nudges. These findings are important since the practice of dark pattern design is common in different platforms across the world [127, 48, 48] and many individuals are arguably influenced by them. For example, in the Cambridge Analytica case, many users fell prey to a dark pattern and disclosed data while they did not necessarily imply their informed consent. Technology developers should identify design strategies that may harm older populations and find practices that facilitate older adults' technological interactions.

In chapter 6, I contribute to this narrative further by showing that part of the different privacy decision-making between younger and older adults can be traced down to having different levels of privacy literacy. Older adults have higher levels of privacy literacy, which leads them to spend more effort on their privacy decisions, and only disclose data if they expect a high value from disclosure.

Furthermore, I showed that older adults have higher levels of privacy concerns. Literature suggests privacy concerns as one of the main concerns for older adults when using the technology [215, 68, 81]. This high level of privacy concerns may also be the main reason for older adults' lack of technology adoption [171]. My results show that older adults' higher privacy concerns translate into their perceptions of risks, benefits, and values of information disclosure. Technology designers should adopt concern-alleviating strategies to reduce costs for older adults. For example, chapter 5 shows that honest communication of the shortcomings of a given product can alleviate older adults' concerns for privacy. However, chapter chapter 6 shows that perceiving disclosure as beneficial can reduce the effect of privacy concerns on disclosure. Therefore, platform designers must communicate the benefits of disclosure, especially to the concerned users. For example, consent notices must explain the benefits of disclosure clearly.

While my studies only focus on the older adult population, future research should study diverse populations and the legislative bodies should specifically consider these diverse populations when imposing new legislation.

7.2 The Dual-route Approach

I used the dual-route privacy framework in this dissertation to study older adults' privacy decision-making. I showed that neither privacy calculus [274, 267] nor the heuristic account [22] solely show the broader picture. Instead of being driven only by heuristics or calculus, privacy decisions are a byproduct of a dual-route process, with decisions concurrently being influenced by both heuristic and conscious elements.

7.2.1 A Framework for Studying Underserved Populations

The dual-route framework is valuable for uncovering the differences in decision-making between populations. This approach teases the decision-making process into smaller components (i.e., heuristic and rational). This divide-and-conquer helps us study and compare different populations concerning their approach to each of the smaller components. Building on this work, scholars can use the dual-route privacy framework to study other populations that are often neglected in technology design (e.g., teens, gender and racial minorities). This approach can help the scientific community and the industry better understand these underserved groups and accommodate them in the design of technology.

7.2.2 Attitudinal vs. Behavioral Effects

Another benefit of using the dual-route privacy framework is that it helped me uncover both the attitudinal and behavioral effects of heuristic (e.g., nudges) and cognitive (e.g., relevance) design interventions. Researchers who only study privacy using heuristic frameworks may neglect to measure different attitudes relating to rational frameworks (e.g., privacy literacy). By having both heuristic and rational frameworks in mind, one can see the bigger picture and study how the elements of the two frameworks may interplay. For example, behavioral economic scholars show how nudges can increase users' disclosure behaviors chapter 3. However, the attitudinal effects of nudges are not well-studied in the literature. In chapter 5 I show that the attitudinal effects of heuristic design interventions are unique from the behavioral effects. For example, a positive default increases disclosure but may make users more cautious. While I used a web-based interface in my studies, future studies can use the dual-route approach while studying other technologies. For example, in a VR setting, scholars can measure not only users' attitudes but also users' emotions using different bodily sensors and use both attitudinal and sensory data for predicting users' behaviors.

7.2.3 Ecological Validity

All the studies in this dissertation were carried out with realistic scenarios where participants thought they were disclosing real data. However, scholars sometimes use hypothetical scenarios to study human behaviors. In contrast to realistic scenarios that measure the actual behavior, hypothetical scenarios ask participants to imagine a situation where they can disclose data and specify their disclosure intentions. While I do not want to undermine the contributions of studies with hypothetical scenarios, the results of realistic studies are more reliable. A common criticism of hypothetical scenarios is that the measured intentions do not necessarily agree with the actual behaviors. In a hypothetical scenario, individuals know that they are not making an actual decision. Without any real consequences, they do not put as much effort into it as they may in an actual situation. In contrast, those who participate in realistic scenarios believe that their decisions will lead to actual consequences. Therefore, realistic scenarios can represent real-world situations better.

Operationalizing privacy studies using realistic scenarios is especially crucial when scholars study privacy by the dual-route approach of rational vs. heuristic. If the experimenter asks participants to "imagine" themselves in a situation and focuses on "thinking" too much, it may nudge participants to use the rational route. Furthermore, heuristic manipulations are subtle and should be hidden from the participants. Therefore, in a hypothetical study and without specific instructions, participants who know their decisions do not have real consequences may not be motivated to invest any effort and submit to heuristics. This can exaggerate the effects of heuristic manipulations in hypothetical scenarios.

7.3 Limitations and Future Work

The contributions of this dissertation should be discussed in light of its limitations. While I used diverse scenarios in this dissertation, we should be cautious in generalizing the findings. For example, it is possible that a certain subgroup of the population is interested in the scenarios (e.g., food recipe and credit recommender). Furthermore, I only studied a US-based population in these studies. Research shows that different cultures have unique privacy attitudes and behaviors [195, 114]. Future studies should investigate if different cultures, for example, are more likely to use a specific route (privacy calculus vs. heuristics) and if the moderators I studied here (e.g., privacy literacy) change per culture. In addition, this document focused on older adults' privacy decision-making mechanism and how it differs from younger adults. Consequently, I only studied these two populations. However, age can be treated as a continuous variable, and future scholars can study participants of all ages and see whether the findings of this study can be replicated with a numeric and linear age variable.

Lastly, future research should study older adults who are non-technology users and explore the technology-avoidance causes among them. My results suggest that older adults who are technology users are worried about their privacy when interacting with technology. It is informative to see if the same privacy concern is prevalent among non-technology-user older adults.

Appendices

Appendix A Supplement Materials For Chapter 6

The instruments for measuring digital privacy literacy:

1- What does the term ”browsing history” stand for? In the browsing history. . .

A. ...the URLs of visited websites are stored.

B. ...cookies from visited websites are stored.

C. ...potentially infected websites are stored separately.

D. ...different information about the user are stored, depending on the browser type.

2- What is a ”cookie”?

A. A text file that enables websites to recognize a user when revisiting.

B. A program to disable data collection from online operators.

C. A computer virus that can be transferred after connecting to a website.

D. A browser plugin that ensures safe online surfing.

3- What does the term ”cache” mean?

A. A buffer memory that accelerates surfing on the Internet.

B. A program that specifically collects information about an Internet user and passes them on to third parties.

C. A program, that copies data on an external hard drive to protect against data theft.

D. A browser plugin that encrypts data transfer when surfing online.

4- What is a ”trojan”? A trojan is a computer program, that. . .

A. ...is disguised as a useful application, but fulfills another function in the background.

B. ...protects a computer from viruses and other malware.

C. ... was developed for fun an d has no specific function.

D. ... caused damage as computer virus in the 90ies but doesn’t exist anymore.

5- What is a ”firewall”?

A. A fallback system that will protect the computer from unwanted web attacks.

B. An outdated protection program against computer viruses

C. A browser plugin that ensures safe online surfing.

D. A new technical development that prevents data loss in case of a short circuit.

6- What is a ”Functional cookie”?

A. Cookies that can remember your preferences to boost the user experience on a website.

B. Cookies that are used to target advertising to a user.

C. A computer program that can upload all the files from your hard drive to the internet.

D. Cookies that allow services to understand how users interact with a particular service.

7-What is a "Marketing cookie"?

A. Cookies that are used to target advertising to a user.

B. Cookies that can remember your preferences to boost the user experience on a website.

C. A computer program that can upload all the files from your hard drive to the internet.

D. Cookies that allow services to understand how users interact with a particular service.

Bibliography

[1] Alessandro Acquisti. Nudging privacy: The behavioral economics of personal information. *IEEE security & privacy*, 7(6):82–85, 2009.

[2] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, et al. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)*, 50(3):1–41, 2017.

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

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

[5] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. Privacy and behavioral economics. In *Modern Socio-Technical Perspectives on Privacy*, pages 61–77. Springer, Cham, 2022.

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

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

[8] Alessandro Acquisti, Leslie K John, and George Loewenstein. What is privacy worth? *The Journal of Legal Studies*, 42(2):249–274, 2013.

[9] Idris Adjerid, Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. Sleights of privacy: Framing, disclosures, and the limits of transparency. In *Proceedings of the ninth symposium on usable privacy and security*, pages 1–11, 2013.

[10] Ritu Agarwal, Vallabh Sambamurthy, and Ralph M Stair. The evolving relationship between general and specific computer self-efficacy—an empirical assessment. *Information systems research*, 11(4):418–430, 2000.

[11] Ben Agger. *Oversharing: Presentations of self in the internet age.* Routledge, 2012.

[12] Ben Agger. *Speeding up fast capitalism: Cultures, jobs, families, schools, bodies.* Routledge, 2015.

[13] Elizabeth Aguirre, Anne L Roggeveen, Dhruv Grewal, and Martin Wetzels. The personalization-privacy paradox: implications for new media. *Journal of Consumer Marketing*, 2016.

[14] Icek Ajzen. Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior 1. *Journal of applied social psychology*, 32(4):665–683, 2002.

[15] Syed H Akhter. Privacy concern and online transactions: the impact of internet self-efficacy and internet involvement. *Journal of Consumer Marketing*, 2014.

[16] Leopoldo Abad Alcalá. Media literacy for older people facing the digital divide: The e-inclusion programmes design. *Comunicar. Media Education Research Journal*, 22(1), 2014.

[17] Ashwaq Alsoubai, Reza Ghaiumy Anaraky, Yao Li, Xinru Page, Bart Knijnenburg, and Pamela J Wisniewski. Permission vs. app limiters: Profiling smartphone users to understand differing strategies for mobile privacy management. In *CHI Conference on Human Factors in Computing Systems*, pages 1–18, 2022.

[18] Irwin Altman. The environment and social behavior: privacy, personal space, territory, and crowding. 1975.

[19] Reza Ghaiumy Anaraky, Paritosh Bahirat, Moloud Nasiri, Xinru Page, Bart P Knijnenburg, and Andrew T Duchowski. Effect of priming on smart home privacy preferences.

[20] Reza Ghaiumy Anaraky, Kaileigh A. Byrne, Pamela J. Wisniewski, Xinru Page, and Bart P. Knijnenburg. To disclose or not to disclose: Examining the privacy decision-making processes of older vs. younger adults. In *To Appear - Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, 2021.

[21] Reza Ghaiumy Anaraky, David Cherry, Marie Jarrell, and Bart Knijnenburg. Testing a comic-based privacy policy. In *The 15th Symposium on Usable Privacy and Security*, 2019.

[22] Reza Ghaiumy Anaraky, Bart P Knijnenburg, and Marten Risius. Exacerbating mindless compliance: The danger of justifications during privacy decision making in the context of facebook applications. *AIS Transactions on Human-Computer Interaction*, 12(2):70–95, 2020.

[23] Reza Ghaiumy Anaraky, Tahereh Nabizadeh, Bart P Knijnenburg, and Marten Risius. Reducing default and framing effects in privacy decision-making. *Proceedings of the Special Interest Group On Humancomputer Interaction*, 2018.

[24] Perrin Andrew Anderson, Monica. The u.s. joins other countries with large aging populations, 2017.

[25] Corey M Angst and Ritu Agarwal. Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS quarterly*, pages 339–370, 2009.

[26] Solomon E Asch. Studies of independence and conformity: I. a minority of one against a unanimous majority. *Psychological monographs: General and applied*, 70(9):1, 1956.

[27] Naveen Farag Awad and M. S. Krishnan. The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization on JSTOR. *MIS Quarterly*, 30(1):13–28, Mar 2006.

[28] Icek Azjen. Understanding attitudes and predicting social behavior. *Englewood Cliffs*, 1980.

[29] Paritosh Bahirat, Martijn C. Willemsen, Yangyang He, Qizhang Sun, and Bart P. Knijnenburg. Overlooking context: How do defaults and framing reduce deliberation in smart home privacy decision-making? In *To Appear - Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, 2021.

[30] Rebecca Balebako, Pedro G Leon, Hazim Almuhimedi, Patrick Gage Kelley, Jonathan Mugan, Alessandro Acquisti, Lorrie Cranor, and Norman Sadeh-Koniecpol. Nudging users towards privacy on mobile devices. 2011.

[31] Paul B Baltes. On the incomplete architecture of human ontogeny: Selection, optimization, and compensation as foundation of developmental theory. *American psychologist*, 52(4):366, 1997.

[32] Ruwan Bandara, Mario Fernando, and Shahriar Akter. Explicating the privacy paradox: A qualitative inquiry of online shopping consumers. *Journal of Retailing and Consumer Services*, 52:101947, 2020.

[33] Albert Bandura. Reflections on self-efficacy. *Advances in behaviour research and therapy*, 1(4):237–269, 1978.

[34] Albert Bandura. Health promotion from the perspective of social cognitive theory. *Psychology and health*, 13(4):623–649, 1998.

[35] Albert Bandura and Sebastian Wessels. Self-efficacy, 1994.

[36] Gaurav Bansal and Fatemeh Zahedi. The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: A multiple-context investigation. *ICIS 2008 Proceedings*, page 7, 2008.

[37] Gaurav Bansal, Fatemeh'Mariam' Zahedi, and David Gefen. The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems*, 24(6):624–644, 2015.

[38] Susan B Barnes. A privacy paradox: Social networking in the united states. *First Monday*, 2006.

[39] Miriam Bartsch and Tobias Dienlin. Control your facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, 56:147–154, 2016.

[40] David Bawden et al. Origins and concepts of digital literacy. *Digital literacies: Concepts, policies and practices*, 30(2008):17–32, 2008.

[41] France Bélanger and Robert E Crossler. Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly*, pages 1017–1041, 2011.

[42] Andrew Besmer, Jason Watson, and Heather Richter Lipford. The impact of social navigation on privacy policy configuration. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, pages 1–10, 2010.

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

[44] James R Bettman, Mary Frances Luce, and John W Payne. Constructive consumer choice processes. *Journal of consumer research*, 25(3):187–217, 1998.

[45] Cabral A Bigman, Joseph N Cappella, and Robert C Hornik. Effective or ineffective: Attribute framing and the human papillomavirus (hpv) vaccine. *Patient education and counseling*, 81:S70–S76, 2010.

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

[47] Borka Jerman Blažič and Andrej Jerman Blažič. Overcoming the digital divide with a modern approach to learning digital skills for the elderly adults. *Education and Information Technologies*, 25(1):259–279, 2020.

[48] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. Tales from the dark side: Privacy dark strategies and privacy dark patterns. *Proceedings on Privacy Enhancing Technologies*, 2016(4):237–254, 2016.

[49] Marc Bourreau, Alexandre De Streel, and Inge Graef. Big data and competition policy: Market power, personalised pricing and advertising. *Personalised Pricing and Advertising (February 16, 2017)*, 2017.

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

[51] Aaron R Brough and Kelly D Martin. Critical roles of knowledge and motivation in privacy research. *Current opinion in psychology*, 31:11–15, 2020.

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

[53] Barry Brown. Studying the internet experience. *HP laboratories technical report HPL*, 49, 2001.

[54] James Dean Brown. The cronbach alpha reliability estimate. *JALT Testing & Evaluation SIG Newsletter*, 6(1), 2002.

[55] Tom Buchanan, Phillip Sainter, and Gunter Saunders. Factors affecting faculty use of learning technologies: Implications for models of technology adoption. *Journal of Computing in Higher education*, 25(1):1–11, 2013.

[56] Christoph Buck, Tamara Dinev, and Reza Ghaiumy Anaraky. Revisiting apco. In *Modern Socio-Technical Perspectives on Privacy*, pages 43–60. Springer, Cham, 2022.

[57] US Census Bureau. Historical Living Arrangements of Adults. Section: Government.

[58] Kaileigh Byrne, Reza Ghaiumy Anaraky, Hannah Barfield, and Summerlin Nickel. Understanding racial and rural disparities in the relationship between social isolation and social technology use. *Innovation in Aging*, 5(Suppl 1):925, 2021.

[59] Kaileigh A Byrne, Reza Ghaiumy Anaraky, Cheryl Dye, Lesley A Ross, Kapil Chalil Madathil, Bart Knijnenburg, and Sue Levkoff. Examining rural and racial disparities in the relationship between loneliness and social technology use among older adults. *Frontiers in Public Health*, 9:723925, 2021.

[60] Kaileigh A Byrne and Reza Ghaiumy Anaraky. Strive to win or not to lose? age-related differences in framing effects on effort-based decision-making. *The Journals of Gerontology: Series B*, 2019.

[61] Kaileigh A Byrne and Reza Ghaiumy Anaraky. Strive to win or not to lose? age-related differences in framing effects on effort-based decision-making. *The Journals of Gerontology: Series B*, 75(10):2095–2105, 2020.

[62] Kaileigh A Byrne and Reza Ghaiumy Anaraky. Identifying racial and rural disparities of cognitive functioning among older adults: The role of social isolation and social technology use. *The Journals of Gerontology: Series B*, 2022.

[63] Carole Cadwalladr and Emma Graham-Harrison. Revealed: 50 million facebook profiles harvested for cambridge analytica in major data breach. *The guardian*, 17:22, 2018.

[64] JD Carpentieri, Jane Elliott, Caroline E Brett, and Ian J Deary. Adapting to aging: Older people talk about their use of selection, optimization, and compensation to maximize well-being in the context of physical decline. *The Journals of Gerontology: Series B*, 72(2):351–361, 2017.

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

[66] J Alberto Castañeda, Francisco J Montoso, and Teodoro Luque. The dimensionality of customer privacy concern on the internet. *Online Information Review*, 2007.

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

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

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

[70] Ramnath K Chellappa and Raymond G Sin. Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information technology and management*, 6(2):181–202, 2005.

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

[72] Hsuan-Ting Chen. Revisiting the privacy paradox on social media with an extended privacy calculus model: The effect of privacy concerns, privacy self-efficacy, and social capital on privacy management. *American behavioral scientist*, 62(10):1392–1412, 2018.

[73] Hsuan-Ting Chen and Wenhong Chen. Couldn't or wouldn't? the influence of privacy concerns and self-efficacy in privacy management on privacy protection. *Cyberpsychology, Behavior, and Social Networking*, 18(1):13–19, 2015.

[74] Hichang Cho and Anna Filippova. Networked privacy management in facebook: A mixed-methods and multinational study. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, pages 503–514, 2016.

[75] Kwok Choon and Mary Jane. Revisiting the privacy paradox on social media: An analysis of privacy practices associated with facebook and twitter. *Canadian Journal of Communication*, 43(2), 2018.

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

[77] Robert B Cialdini. The psychology of persuasion. *New York*, 1993.

[78] Robert B Cialdini, Linda J Demaine, Brad J Sagarin, Daniel W Barrett, Kelton Rhoads, and Patricia L Winter. Managing social norms for persuasive impact. *Social influence*, 1(1):3–15, 2006.

[79] Robert B Cialdini, Carl A Kallgren, and Raymond R Reno. A focus theory of normative conduct: A theoretical refinement and reevaluation of the role of norms in human behavior. In *Advances in experimental social psychology*, volume 24, pages 201–234. Elsevier, 1991.

[80] Robert B Cialdini, Raymond R Reno, and Carl A Kallgren. A focus theory of normative conduct: Recycling the concept of norms to reduce littering in public places. *Journal of personality and social psychology*, 58(6):1015, 1990.

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

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

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

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

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

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

[87] Adrian Dabrowski, Georg Merzdovnik, Johanna Ullrich, Gerald Sendera, and Edgar Weippl. Measuring cookies and web privacy in a post-gdpr world. In *International Conference on Passive and Active Network Measurement*, pages 258–270. Springer, 2019.

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

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

[90] Kenan Degirmenci. Mobile users’ information privacy concerns and the role of app permission requests. *International Journal of Information Management*, 50:261–272, 2020.

[91] Chrysanthos Dellarocas, Xiaoquan Michael Zhang, and Neveen F Awad. Exploring the value of online product reviews in forecasting sales: The case of motion pictures. *Journal of Interactive marketing*, 21(4):23–45, 2007.

[92] Miriam K Depping and Alexandra M Freund. Normal aging and decision making: The role of motivation. *Human Development*, 54(6):349–367, 2011.

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

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

[95] Tamara Dinev, Allen R McConnell, and H Jeff Smith. Research commentary—informing privacy research through information systems, psychology, and behavioral economics: thinking outside the "apco" box. *Information Systems Research*, 26(4):639–655, 2015.

[96] Isaac Dinner, Eric J Johnson, Daniel G Goldstein, and Kaiya Liu. Partitioning default effects: why people choose not to choose. *Journal of Experimental Psychology: Applied*, 17(4):332, 2011.

[97] Curt J Dommeyer and Barbara L Gross. What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies. *Journal of Interactive Marketing*, 17(2):34–51, 2003.

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

[99] Wenjing Duan, Bin Gu, and Andrews B Whinston. Analysis of herding on the internet-an empirical investigation of online software download. *AMCIS 2005 Proceedings*, page 488, 2005.

[100] Mary Ann Eastlick, Sherry L Lotz, and Patricia Warrington. Understanding online b-to-c relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of business research*, 59(8):877–886, 2006.

[101] Steven M Edwards, Hairong Li, and Joo-Hyun Lee. Forced exposure and psychological reactance: Antecedents and consequences of the perceived intrusiveness of pop-up ads. *Journal of advertising*, 31(3):83–95, 2002.

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

[103] Kelwin Fernandes, Pedro Vinagre, and Paulo Cortez. A proactive intelligent decision support system for predicting the popularity of online news. In *Portuguese Conference on Artificial Intelligence*, pages 535–546. Springer, 2015.

[104] Harvey V Fineberg. Retooling for an aging america. *The Medscape Journal of Medicine*, 10(8):188, 2008.

[105] AD Fisk and Rogers WA. Charness n./czaja sj/sharit j.(2009): Designing for older adults. principles and creative human factor approaches.

[106] Elizabeth Ford, Keegan Curlewis, Akkapon Wongkoblap, and Vasa Curcin. Public opinions on using social media content to identify users with depression and target mental health care advertising: mixed methods survey. *JMIR mental health*, 6(11):e12942, 2019.

[107] Grace Fox and Regina Connolly. Mobile health technology adoption across generations: Narrowing the digital divide. *Information Systems Journal*, 28(6):995–1019, 2018.

[108] Sandra Freitas, Mário R Simões, Lara Alves, and Isabel Santana. Montreal cognitive assessment (moca): normative study for the portuguese population. *Journal of clinical and experimental neuropsychology*, 33(9):989–996, 2011.

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

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

[111] Eyal Gamliel and Eyal Peer. Attribute framing affects the perceived fairness of health care allocation principles. *Judgment and Decision Making*, 5(1):11, 2010.

[112] Maria Gardiner, Mary A Luszcz, and Janet Bryan. The manipulation and measurement of task-specific memory self-efficacy in younger and older adults. *International Journal of Behavioral Development*, 21(2):209–228, 1997.

[113] Reza Ghaiumy Anaraky and Bart Knijnenburg. A research agenda for studying young and older adults' privacy decisions. *Bart, A Research Agenda for Studying Young and Older Adults' Privacy Decisions (June 25, 2021)*, 2021.

[114] Reza Ghaiumy Anaraky, Yao Li, and Bart Knijnenburg. Difficulties of measuring culture in privacy studies. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2):1–26, 2021.

[115] Thomas Gilovich, D Keltner, and RE Nisbett. Social psychology . new york, ny: W. w, 2010.

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

[117] Avi Goldfarb and Catherine Tucker. Shifts in privacy concerns. *American Economic Review*, 102(3):349–53, 2012.

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

[119] Ralph Gonzales, Tammy Anderer, Charles E McCulloch, Judith H Maselli, Frederick J Bloom, Thomas R Graf, Melissa Stahl, Michelle Yefko, Julie Molecavage, and Joshua P Metlay. A cluster randomized trial of decision support strategies for reducing antibiotic use in acute bronchitis. *JAMA internal medicine*, 173(4):267–273, 2013.

[120] Colin M Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L Toombs. The dark (patterns) side of ux design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2018.

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

[122] Anatoliy Gruzd and Ángel Hernández-García. Privacy concerns and self-disclosure in private and public uses of social media. *Cyberpsychology, Behavior, and Social Networking*, 21(7):418–428, 2018.

[123] Lijie Guo, Christopher Flathmann, Reza Anaraky, Nathan McNeese, and Bart Knijnenburg. The effect of recommendation source and justification on professional development recommendations for high school teachers. In *Proceedings of the 33rd ACM Conference on Hypertext and Social Media*, pages 175–185, 2022.

[124] Loni Hagen. Overcoming the privacy challenges of wearable devices: A study on the role of digital literacy. In *Proceedings of the 18th Annual International Conference on Digital Government Research*, pages 598–599, 2017.

[125] Keith N Hampton, Lauren Sessions Goulet, Cameron Marlow, and Lee Rainie. Why most facebook users get more than they give. *Pew Internet & American Life Project*, 3(2012):1–40, 2012.

[126] Ward A Hanson and Daniel S Putler. Hits and misses: Herd behavior and online product popularity. *Marketing letters*, 7(4):297–305, 1996.

[127] Jeremy Rosenberg Harry Brignull, Marc Miquel and James Offer. Dark patterns - user interfaces designed to trick people., 2015.

[128] Peter A Heslin and Ute-Christine Klehe. Self-efficacy. *Encyclopedia Of Industrial/Organizational Psychology, SG Rogelberg, ed*, 2:705–708, 2006.

[129] Thomas M Hess. Selective engagement of cognitive resources: Motivational influences on older adults' cognitive functioning. *Perspectives on Psychological Science*, 9(4):388–407, 2014.

[130] Cho Hichang. Determinants of behavioral responses to online privacy: The effects of concern, risk beliefs, self-efficacy, and communication sources on self-protection strategies. *Journal of Information Privacy and Security*, 6(1):3–27, 2010.

[131] E Tory Higgins and John A Bargh. Social cognition and social perception. *Annual review of psychology*, 38(1):369–425, 1987.

[132] Rudy Hirschheim. Against theory: With apologies to feyerabend. *Journal of the Association for Information Systems*, 20(9):8, 2019.

[133] Christian Pieter Hoffmann and Christoph Lutz. Digital divides in political participation: The mediating role of social media self-efficacy and privacy concerns. *Policy & Internet*, 13(1):6–29, 2021.

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

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

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

[137] Jen-Hung Huang and Yi-Fen Chen. Herding in online product choice. *Psychology & Marketing*, 23(5):413–428, 2006.

[138] Gordon Hull, Heather Richter Lipford, and Celine Latulipe. Contextual gaps: privacy issues on facebook. *Ethics and information technology*, 13(4):289–302, 2011.

[139] Athina Ioannou, Iis Tussyadiah, and Yang Lu. Privacy concerns and disclosure of biometric and behavioral data for travel. *International Journal of Information Management*, 54:102122, 2020.

[140] Ganesh Iyer, David Soberman, and J Miguel Villas-Boas. The targeting of advertising. *Marketing Science*, 24(3):461–476, 2005.

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

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

[143] Haiyan Jia and Heng Xu. Measuring individuals' concerns over collective privacy on social networking sites. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 10(1), 2016.

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

[145] Surej P John. Influence of computer self-efficacy on information technology adoption. *International Journal of Information Technology*, 19(1):1–13, 2013.

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

[147] Eric J Johnson, Simon Gächter, and Andreas Herrmann. Exploring the nature of loss aversion. 2006.

[148] Eric J Johnson and Daniel Goldstein. Do defaults save lives?, 2003.

[149] Eric J Johnson, John Hershey, Jacqueline Meszaros, and Howard Kunreuther. Framing, probability distortions, and insurance decisions. *Journal of risk and uncertainty*, 7(1):35–51, 1993.

[150] Eric J Johnson, Suzanne B Shu, Benedict GC Dellaert, Craig Fox, Daniel G Goldstein, Gerald Häubl, Richard P Larrick, John W Payne, Ellen Peters, David Schkade, et al. Beyond nudges: Tools of a choice architecture. *Marketing Letters*, 23(2):487–504, 2012.

[151] Adam N Joinson, Ulf-Dietrich Reips, Tom Buchanan, and Carina B Paine Schofield. Privacy, trust, and self-disclosure online. *Human–Computer Interaction*, 25(1):1–24, 2010.

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

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

[154] Jaehyeon Ju, Youngsok Bang, Dong-joo Lee, and Jae-Hyeon Ahn. Benefit ambiguity and asymmetric herding in privacy decisions: A field experiment in a mobile application system. 2019.

[155] Daniel Kahneman, Jack L Knetsch, and Richard H Thaler. Anomalies: The endowment effect, loss aversion, and status quo bias. *Journal of Economic perspectives*, 5(1):193–206, 1991.

[156] Daniel Kahneman, Jack L Knetsch, and Richard H Thaler. The endowment effect, loss aversion, and status quo bias: Anomalies. *Journal of Economic perspectives*, 5(1):193–206, 1991.

[157] D Kahnemann. choices, values, and frames, american psychologist, 39, 1984.

[158] Carl A Kallgren, Raymond R Reno, and Robert B Cialdini. A focus theory of normative conduct: When norms do and do not affect behavior. *Personality and social psychology bulletin*, 26(8):1002–1012, 2000.

[159] Amanda Kearney. *Uses and gratification of posting selfies on social media.* Rochester Institute of Technology, 2018.

[160] Flavius Kehr, Tobias Kowatsch, Daniel Wentzel, and Elgar Fleisch. Thinking styles and privacy decisions: need for cognition, faith into intuition, and the privacy calculus. 2015.

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

[162] Gideon Keren. Framing, intentions, and trust–choice incompatibility. *Organizational Behavior and Human Decision Processes*, 103(2):238–255, 2007.

[163] Murat Kezer, Barış Sevi, Zeynep Cemalcilar, and Lemi Baruh. Age differences in privacy attitudes, literacy and privacy management on facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 10(1), 2016.

[164] HyeKyoung Kim and Jihoon Song. The quality of word-of-mouth in the online shopping mall. *Journal of Research in Interactive Marketing*, 2010.

[165] Tom W Kirkman. Statistics to use. *http://www. physics. csbsju. edu/stats/*, 1996.

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

[167] Bart P Knijnenburg, Reza Ghaiumy Anaraky, Daricia Wilkinson, Moses Namara, Yangyang He, David Cherry, and Erin Ash. User-tailored privacy. In *Modern Socio-Technical Perspectives on Privacy*, pages 367–393. Springer, Cham, 2022.

[168] Bart P Knijnenburg and Alfred Kobsa. Making decisions about privacy: information disclosure in context-aware recommender systems. *ACM Transactions on Interactive Intelligent Systems (TiiS)*, 3(3):1–23, 2013.

[169] Bart Piet Knijnenburg and Alfred Kobsa. Increasing sharing tendency without reducing satisfaction: Finding the best privacy-settings user interface for social networks. In *ICIS*, 2014.

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

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

[172] Alfred Kobsa, Hichang Cho, and Bart P Knijnenburg. The effect of personalization provider characteristics on privacy attitudes and behaviors: An e laboration l ikelihood m odel approach. *Journal of the Association for Information Science and Technology*, 67(11):2587–2606, 2016.

[173] Jan Kolter, Thomas Kernchen, and Günther Pernul. Collaborative privacy management. *computers & security*, 29(5):580–591, 2010.

[174] Jacob Kramer-Duffield. *Beliefs and uses of tagging among undergraduates.* The University of North Carolina at Chapel Hill, 2010.

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

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

[177] Jess Kropczynski, Reza Ghaiumy Anaraky, Mamtaj Akter, Amy J Godfrey, Heather Lipford, and Pamela J Wisniewski. Examining collaborative support for privacy and security in the broader context of tech caregiving. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2):1–23, 2021.

[178] Robin L. West, Roxanne M. Thorn. Goal-setting, self-efficacy, and memory performance in older and younger adults. *Experimental aging research*, 27(1):41–65, 2001.

[179] Yee-Lin Lai and Kai-Lung Hui. Internet opt-in and opt-out: investigating the roles of frames, defaults and privacy concerns. In *Proceedings of the 2006 ACM SIGMIS CPR conference on computer personnel research: Forty four years of computer personnel research: achievements, challenges & the future*, pages 253–263, 2006.

[180] Francesco Lamonaca, Giuseppe Polimeni, Kurt Barbé, and Domenico Grimaldi. Health parameters monitoring by smartphone for quality of life improvement. *Measurement*, 73:82–94, 2015.

[181] Ellen J Langer. Minding matters: The consequences of mindlessness–mindfulness. In *Advances in experimental social psychology*, volume 22, pages 137–173. Elsevier, 1989.

[182] Ellen J Langer, Arthur Blank, and Benzion Chanowitz. The mindlessness of ostensibly thoughtful action: The role of" placebic" information in interpersonal interaction. *Journal of personality and social psychology*, 36(6):635, 1978.

[183] AJ Larner. Screening utility of the montreal cognitive assessment (moca): in place of-or as well as-the mmse? *International Psychogeriatrics*, 24(3):391, 2012.

[184] Robert LaRose and Nora J Rifon. Promoting i-safety: effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *Journal of Consumer Affairs*, 41(1):127–149, 2007.

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

[186] Scott Lederer, Jennifer Mankoff, and Anind K Dey. Who wants to know what when? privacy preference determinants in ubiquitous computing. In *CHI'03 extended abstracts on Human factors in computing systems*, pages 724–725, 2003.

[187] Hyun-Hwa Lee and Jessica T Hill. Moderating effect of privacy self-efficacy on location-based mobile marketing. *International Journal of Mobile Communications*, 11(4):330–350, 2013.

[188] Kevin Levitt, Jeremy Edwards, Chi-Ming Chow, and R Sacha Bhatia. Development of an educational strategy and decision support tool to enhance appropriate use of stress echocardiography at a large academic medical center: a prospective, pre-and postintervention analysis. *Journal of the American Society of Echocardiography*, 28(12):1401–1409, 2015.

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

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

[191] Bin Li. The classical model of decision making has been accepted as not providing an accurate account of how people typically make decisions. *International Journal of Business and management*, 3(6):151–154, 2008.

[192] Chia-Ying Li. Persuasive messages on information system acceptance: A theoretical extension of elaboration likelihood model and social influence theory. *Computers in Human Behavior*, 29(1):264–275, 2013.

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

[194] Yao Li, Hichang Cho, Reza Ghaiumy Anaraky, Bart Knijnenburg, and Alfred Kobsa. Antecedents of collective privacy management in social network sites: a cross-country analysis. *CCF Transactions on Pervasive Computing and Interaction*, pages 1–18, 2022.

[195] Yao Li, Reza Ghaiumy Anaraky, and Bart Knijnenburg. How not to measure social network privacy: A cross-country investigation. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW1):1–32, 2021.

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

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

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

[199] Lesa Lorenzen-Huber, Mary Boutain, L Jean Camp, Kalpana Shankar, and Kay H Connelly. Privacy, technology, and aging: A proposed framework. *Ageing International*, 36(2):232–252, 2011.

[200] Andreas Lymberis. Smart wearables for remote health monitoring, from prevention to rehabilitation: current r&amp;d, future challenges. In *4th International IEEE EMBS Special Topic Conference on Information Technology Applications in Biomedicine, 2003.*, pages 272–275. IEEE, 2003.

[201] Aditi M. Bhoot, Mayuri A. Shinde, and Wricha P. Mishra. Towards the identification of dark patterns: An analysis based on end-user reactions. In *IndiaHCI'20: Proceedings of the 11th Indian Conference on Human-Computer Interaction*, pages 24–33, 2020.

[202] Brigitte C Madrian and Dennis F Shea. The power of suggestion: Inertia in 401 (k) participation and savings behavior. *The Quarterly journal of economics*, 116(4):1149–1187, 2001.

[203] Stefan Mager and Johann Kranz. On the effectiveness of overt and covert interventions in influencing cookie consent: Field experimental evidence. 2021.

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

[205] Naresh K Malhotra, Sung S Kim, and James Agarwal. Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model. *Information systems research*, 15(4):336–355, 2004.

[206] Isabel Marcin and Andreas Nicklisch. Testing the endowment effect for default rules. *Review of Law & Economics*, 13(2), 2017.

[207] Philipp K Masur, Doris Teutsch, and Sabine Trepte. Entwicklung und validierung der online-privatheitskompetenzskala (oplis). *Diagnostica*, 2017.

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

[209] Mara Mather, Nina Mazar, Marissa A Gorlick, Nichole R Lighthall, Jessica Burgeno, Andrej Schoeke, and Dan Ariely. Risk preferences and aging: The "certainty effect" in older adults' decision making. *Psychology and aging*, 27(4):801, 2012.

[210] Arunesh Mathur, Gunes Acar, Michael J Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. Dark patterns at scale: Findings from a crawl of 11k shopping websites. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–32, 2019.

[211] Arunesh Mathur, Jonathan Mayer, and Mihir Kshirsagar. What makes a dark pattern... dark? design attributes, normative considerations, and measurement methods. *arXiv preprint arXiv:2101.04843*, 2021.

[212] Aleecia M McDonald and Lorrie Faith Cranor. Americans' attitudes about internet behavioral advertising practices. In *Proceedings of the 9th annual ACM workshop on Privacy in the electronic society*, pages 63–72, 2010.

[213] Craig RM McKenzie, Michael J Liersch, and Stacey R Finkelstein. Recommendations implicit in policy defaults. *Psychological Science*, 17(5):414–420, 2006.

[214] D Harrison McKnight, Vivek Choudhury, and Charles Kacmar. Developing and validating trust measures for e-commerce: An integrative typology. *Information systems research*, 13(3):334–359, 2002.

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

[216] Andrew L Mendelson and Zizi Papacharissi. Look at us: Collective narcissism in college student facebook photo galleries. *The networked self: Identity, community and culture on social network sites*, 1974:1–37, 2010.

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

[218] Miriam J Metzger. Effects of site, vendor, and consumer characteristics on web site trust and disclosure. *Communication Research*, 33(3):155–179, 2006.

[219] Stanley Milgram. Behavioral study of obedience. *The Journal of abnormal and social psychology*, 67(4):371, 1963.

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

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

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

[223] Sunil Mithas, Jiban Khuntia, and Ritu Agarwal. Information technology and life expectancy: A country-level analysis. 2009.

[224] Vivian Genaro Motti and Kelly Caine. Users' privacy concerns about wearables. In *International Conference on Financial Cryptography and Data Security*, pages 231–244. Springer, 2015.

[225] Bengt Muthén and Linda Muthén. *Mplus*. Chapman and Hall/CRC, 2017.

[226] Moses Namara, Reza Ghaiumy Anaraky, Pamela Wisniewski, Xinru Page, and Bart P Knijnenburg. Examining power use and the privacy paradox between intention vs. actual use of mobile applications. In *European Symposium on Usable Security 2021*, pages 223–235, 2021.

[227] United Nations. Ageing.

[228] Xaver Neumeyer, Susana C Santos, and Michael H Morris. Overcoming barriers to technology adoption when fostering entrepreneurship among the poor: the role of technology and digital literacy. *IEEE Transactions on Engineering Management*, 2020.

[229] Barbara M Newman and Philip R Newman. *Development through life: A psychosocial approach*. Cengage Learning, 2017.

[230] Nicholas R Nicholson. A review of social isolation: an important but underassessed condition in older adults. *The journal of primary prevention*, 33(2-3):137–152, 2012.

[231] Helen Nissenbaum. Privacy as contextual integrity. *Wash. L. Rev.*, 79:119, 2004.

[232] Patricia A Norberg, Daniel R Horne, and David A Horne. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of consumer affairs*, 41(1):100–126, 2007.

[233] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. Dark patterns after the gdpr: Scraping consent pop-ups and demonstrating their influence. In *Proceedings of the 2020 CHI conference on human factors in computing systems*, pages 1–13, 2020.

[234] JC Nunnally. Psychometric theory 2nd edition (new york: Mcgraw). 1978.

[235] US Department of Health, Human Services, et al. Administration on aging. 2017 profile of older americans, 2019.

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

[237] Xinru Page, Reza Ghaiumy Anaraky, and Bart P Knijnenburg. How communication style shapes relationship boundary regulation and social media adoption. In *Proceedings of the 10th International Conference on Social Media and Society*, pages 126–135, 2019.

[238] Xinru Page, Reza Ghaiumy Anaraky, Bart P Knijnenburg, and Pamela J Wisniewski. Pragmatic tool vs. relational hindrance: Exploring why some social media users avoid privacy features. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–23, 2019.

[239] Xinru Page and Marco Marabelli. Changes in social media behavior during life periods of uncertainty. In *Proceedings of the International AAAI Conference on Web and Social Media*, volume 11, 2017.

[240] Leysia Palen and Paul Dourish. Unpacking" privacy" for a networked world. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 129–136, 2003.

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

[242] Greig Paul and James Irvine. Privacy implications of wearable health devices. In *Proceedings of the 7th International Conference on Security of Information and Networks*, pages 117–121, 2014.

[243] Paul A Pavlou, Huigang Liang, and Yajiong Xue. Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS quarterly*, pages 105–136, 2007.

[244] Tiffany A Pempek, Yevdokiya A Yermolayeva, and Sandra L Calvert. College students' social networking experiences on facebook. *Journal of applied developmental psychology*, 30(3):227–238, 2009.

[245] Caitlin Petre. Engineering consent: How the design and marketing of newsroom analytics tools rationalize journalists' labor. *Digital Journalism*, 6(4):509–527, 2018.

[246] Richard E Petty and Pablo Briñol. The elaboration likelihood model. *Handbook of theories of social psychology*, 1:224–245, 2011.

[247] Richard E Petty and John T Cacioppo. The elaboration likelihood model of persuasion. In *Communication and persuasion*, pages 1–24. Springer, 1986.

[248] Matthew Pittman and Brandon Reich. Social media and loneliness: Why an instagram picture may be worth more than a thousand twitter words. *Computers in Human Behavior*, 62:155–167, 2016.

[249] Silvia Puglisi, Javier Parra-Arnau, Jordi Forné, and David Rebollo-Monedero. On content-based recommendation and user privacy in social-tagging systems. *Computer Standards & Interfaces*, 41:17–27, 2015.

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

[251] Justine Rapp, Ronald Paul Hill, Jeannie Gaines, and R Mark Wilson. Advertising and consumer privacy. *Journal of Advertising*, 38(4):51–61, 2009.

[252] Pat Reid. Supporting instructors in overcoming self-efficacy and background barriers to adoption. *Education and Information Technologies*, 22(1):369–382, 2017.

[253] Raymond R Reno, Robert B Cialdini, and Carl A Kallgren. The transsituational influence of social norms. *Journal of personality and social psychology*, 64(1):104, 1993.

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

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

[256] HR Roberts, Jason Bennett Thatcher, and Richard Klein. Using information technology mindfully. In *Proceedings of the 2007 Southern Association for Information Systems Conference*, pages 3–4, 2007.

[257] Salvador Rodriguez. Here are the scandals and other incidents that have sent facebook's share price tanking in 2018. *CNBC. November*, 21, 2018.

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

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

[260] Chris Rose. The security implications of ubiquitous social media. *International Journal of Management & Information Systems (IJMIS)*, 15(1), 2011.

[261] Matthew Rueben, Frank J Bernieri, Cindy M Grimm, and William D Smart. Framing effects on privacy concerns about a home telepresence robot. In *Proceedings of the 2017 ACM/IEEE International Conference on Human-Robot Interaction*, pages 435–444, 2017.

[262] Paul Russo and Oded Nov. Photo tagging over time: A longitudinal study of the role of attention, network density, and motivations. In *Proceedings of the International AAAI Conference on Web and Social Media*, volume 4, 2010.

[263] Sonam Samat and Alessandro Acquisti. Format vs. content: the impact of risk and presentation on disclosure decisions. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*, pages 377–384, 2017.

[264] William Samuelson and Richard Zeckhauser. Status quo bias in decision making. *Journal of risk and uncertainty*, 1(1):7–59, 1988.

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

[266] Mike Schroepfer. An update on our plans to restrict data access on facebook. *Facebook newsroom*, 4, 2018.

[267] John Scott. Rational choice theory. *Understanding contemporary society: Theories of the present*, 129:671–85, 2000.

[268] Hyunjin Seo, Joseph Erba, Mugur V Geana, and Crystal Y Lumpkins. Calling doctor google? technology adoption and health information seeking among low-income african american older adults. 2017.

[269] Leigh S Shaffer. Toward pepitone's vision of a normative social psychology: What is a social norm? *The journal of mind and behavior*, pages 275–293, 1983.

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

[271] Shlomi Sher and Craig RM McKenzie. Information leakage from logically equivalent frames. *Cognition*, 101(3):467–494, 2006.

[272] Hu Shuijing and Jiang Tao. An empirical study on digital privacy risk of senior citizens. In *2017 International Conference on Robots & Intelligent System (ICRIS)*, pages 19–24. IEEE, 2017.

[273] Michael Siegrist and George Cvetkovich. Better negative than positive? evidence of a bias for negative information about possible health dangers. *Risk analysis*, 21(1):199–206, 2001.

[274] Herbert A Simon. A behavioral model of rational choice. *The quarterly journal of economics*, 69(1):99–118, 1955.

[275] GiriBabu Sinnapolu and Shadi Alawneh. Integrating wearables with cloud-based communication for health monitoring and emergency assistance. *Internet of Things*, 1:40–54, 2018.

[276] Edith G Smit, Guda Van Noort, and Hilde AM Voorveld. Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in europe. *Computers in Human Behavior*, 32:15–22, 2014.

[277] H Jeff Smith, Tamara Dinev, and Heng Xu. Information privacy research: an interdisciplinary review. *MIS quarterly*, pages 989–1015, 2011.

[278] N Craig Smith, Daniel G Goldstein, and Eric J Johnson. Choice without awareness: Ethical and policy implications of defaults. *Journal of Public Policy & Marketing*, 32(2):159–172, 2013.

[279] Andrew D Smock, Nicole B Ellison, Cliff Lampe, and Donghee Yvette Wohn. Facebook as a toolkit: A uses and gratification approach to unbundling feature use. *Computers in human behavior*, 27(6):2322–2329, 2011.

[280] Daniel J Solove. Privacy self-management and the consent dilemma, 126 harvard law review 1880, 2013.

[281] Sarah Spiekermann, Alessandro Acquisti, Rainer Böhme, and Kai-Lung Hui. The challenges of personal data markets and privacy. *Electronic markets*, 25(2):161–167, 2015.

[282] Sarah Spiekermann, Jens Grossklags, and Bettina Berendt. E-privacy in 2nd generation e-commerce: privacy preferences versus actual behavior. In *Proceedings of the 3rd ACM conference on Electronic Commerce*, pages 38–47, 2001.

[283] Lucas Spreiter, Annette Isabel Böhmer, Udo Lindemann, et al. Evaluation of taf agile framework based on the development of an innovative emergency wearable for seniors. In *DS 92: Proceedings of the DESIGN 2018 15th International Design Conference*, pages 1345–1356, 2018.

[284] Zak Stone, Todd Zickler, and Trevor Darrell. Autotagging facebook: Social network context improves photo annotation. In *2008 IEEE computer society conference on computer vision and pattern recognition workshops*, pages 1–8. IEEE, 2008.

[285] Stoyan R Stoyanov, Leanne Hides, David J Kavanagh, Oksana Zelenko, Dian Tjondronegoro, and Madhavan Mani. Mobile app rating scale: a new tool for assessing the quality of health mobile apps. *JMIR mHealth and uHealth*, 3(1):e27, 2015.

[286] Fred Stutzman and Jacob Kramer-Duffield. Friends only: examining a privacy-enhancing behavior in facebook. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 1553–1562, 2010.

[287] Heshan Sun and Yulin Fang. Toward a model of mindfulness in technology acceptance. 2010.

[288] Yongqiang Sun, Nan Wang, Xiao-Liang Shen, and Jacky Xi Zhang. Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior*, 52:278–292, 2015.

[289] Juliana Sutanto, Elia Palme, Chuan-Hoo Tan, and Chee Wei Phang. Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users. *MIS quarterly*, pages 1141–1164, 2013.

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

[291] Monika Taddicken. The 'privacy paradox'in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, 19(2):248–273, 2014.

[292] Shalini Talwar, Amandeep Dhir, Puneet Kaur, Nida Zafar, and Melfi Alrasheedy. Why do people share fake news? associations between the dark side of social media use and fake news sharing behavior. *Journal of Retailing and Consumer Services*, 51:72–82, 2019.

[293] Xin Tan, Li Qin, Yongbeom Kim, and Jeffrey Hsu. Impact of privacy concern in social networking web sites. *Internet Research*, 2012.

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

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

[296] Richard H Thaler and Cass R Sunstein. Nudge: Improving decisions about health, wealth, and happiness.

[297] Richard H Thaler, Cass R Sunstein, and John P Balz. Choice architecture. In *The behavioral foundations of public policy*, pages 428–439. Princeton University Press, 2013.

[298] Jason Bennett Thatcher, Ryan T Wright, Heshan Sun, Thomas J Zagenczyk, and Richard Klein. Mindfulness in information technology use: Definitions, distinctions, and a new measure. *MIS Quarterly*, 42(3):831–848, 2018.

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

[300] Eran Toch, Justin Cranshaw, Paul Hankes Drielsma, Janice Y Tsai, Patrick Gage Kelley, James Springfield, Lorrie Cranor, Jason Hong, and Norman Sadeh. Empirical models of privacy in location sharing. In *Proceedings of the 12th ACM international conference on Ubiquitous computing*, pages 129–138, 2010.

[301] Hsin-yi Sandy Tsai, Ruth Shillair, and Shelia R Cotten. Social support and "playing around" an examination of how older adults acquire digital literacy with tablet computers. *Journal of Applied Gerontology*, 36(1):29–55, 2017.

[302] Zeynep Tufekci. Can you see me now? audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, 28(1):20–36, 2008.

[303] Amos Tversky and Daniel Kahneman. The framing of decisions and the psychology of choice. *science*, 211(4481):453–458, 1981.

[304] Amos Tversky and Daniel Kahneman. Rational choice and the framing of decisions. In *Multiple criteria decision making and risk analysis using microcomputers*, pages 81–126. Springer, 1989.

[305] Amos Tversky and Daniel Kahneman. Advances in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and uncertainty*, 5(4):297–323, 1992.

[306] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. (un) informed consent: Studying gdpr consent notices in the field. In *Proceedings of the 2019 acm sigsac conference on computer and communications security*, pages 973–990, 2019.

[307] Evert Van den Broeck, Karolien Poels, and Michel Walrave. 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):2056305115616149, 2015.

[308] Tommaso Venturini and Richard Rogers. "api-based research" or how can digital sociology and journalism studies learn from the facebook and cambridge analytica data breach. *Digital Journalism*, 7(4):532–540, 2019.

[309] Eka Dyar Wahyuni and Arif Djunaidy. Fake review detection from a product review using modified method of iterative computation framework. In *MATEC web of conferences*, volume 58, page 03003. EDP Sciences, 2016.

[310] Cheng-Hui Wang and Chih-Lun Wu. Bridging the digital divide: the smart tv as a platform for digital literacy among the elderly. *Behaviour & Information Technology*, pages 1–14, 2021.

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

[312] Huaiqing Wang, Matthew KO Lee, and Chen Wang. Consumer privacy concerns about internet marketing. *Communications of the ACM*, 41(3):63–70, 1998.

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

[314] Yang Wang, Pedro Giovanni Leon, Alessandro Acquisti, Lorrie Faith Cranor, Alain Forget, and Norman Sadeh. A field trial of privacy nudges for facebook. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 2367–2376, 2014.

[315] Yang Wang, Gregory Norcie, Saranga Komanduri, Alessandro Acquisti, Pedro Giovanni Leon, and Lorrie Faith Cranor. " i regretted the minute i pressed share" a qualitative study of regrets on facebook. In *Proceedings of the seventh symposium on usable privacy and security*, pages 1–16, 2011.

[316] Pei-Shan Wei and Hsi-Peng Lu. An examination of the celebrity endorsements and online customer reviews influence female consumers' shopping behavior. *Computers in Human Behavior*, 29(1):193–201, 2013.

[317] Marc G Weinberger and William R Dillon. The effects of unfavorable product rating information. *ACR North American Advances*, 1980.

[318] Herb Weisbaum. Zuckerberg's apology tour has not done much to regain user trust. *NBC News*, 2018.

[319] A Westin, HARRIS LOUIS, et al. Equifax-harris consumer privacy survey. *Conducted for Equifax Inc*, 1991.

[320] Monica Whitty, James Doodson, Sadie Creese, and Duncan Hodges. Individual differences in cyber security behaviors: an examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking*, 18(1):3–7, 2015.

[321] Katherine V Wild, Nora C Mattek, Shoshana A Maxwell, Hiroko H Dodge, Holly B Jimison, and Jeffrey A Kaye. Computer-related self-efficacy and anxiety in older adults with and without mild cognitive impairment. *Alzheimer's &amp; Dementia*, 8(6):544–552, 2012.

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

[323] Pamela Wisniewski, AKM Islam, Heather Richter Lipford, and David C Wilson. Framing and measuring multi-dimensional interpersonal privacy preferences of social networking site users. *Communications of the Association for information systems*, 38(1):10, 2016.

[324] Pamela Wisniewski, Heng Xu, Heather Lipford, and Emmanuel Bello-Ogunu. F acebook apps and tagging: The trade-off between personal privacy and engaging with friends. *Journal of the Association for Information Science and Technology*, 66(9):1883–1896, 2015.

[325] Christina L Wissinger. Privacy literacy: From theory to practice. *Communications in Information Literacy*, 11(2):378–389, 2017.

[326] Ben Wolford. Knuth: Computers and typesetting.

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

[328] Ya-Huei Wu, Souad Damnée, Helene Kerhervé, Caitlin Ware, and Anne-Sophie Rigaud. Bridging the digital divide in older adults: a study from an initiative to inform older adults about new technologies. *Clinical interventions in aging*, 10:193, 2015.

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

[330] Heng Xu and Sumeet Gupta. The effects of privacy concerns and personal innovativeness on potential and experienced customers' adoption of location-based services. *Electronic Markets*, 19(2-3):137–149, 2009.

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

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

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

[334] Seounmi Youn. Teenagers' perceptions of online privacy and coping behaviors: a risk–benefit appraisal approach. *Journal of Broadcasting &amp; Electronic Media*, 49(1):86–110, 2005.

[335] Tai-Kuei Yu, Mei-Lan Lin, and Ying-Kai Liao. Understanding factors influencing information communication technology adoption behavior: The moderators of information literacy and digital skills. *Computers in Human Behavior*, 71:196–208, 2017.

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

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

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

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

[340] Tomasz Zukowski and Irwin Brown. Examining the influence of demographic factors on internet users' information privacy concerns. In *Proceedings of the 2007 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries*, pages 197–204, 2007.