Can Informational Privacy as a Value be Reliably Measured as a Dimension of Privacy When Studying Differences in Behaviour in German and Romanian people

Matthias Giesen

S2557479

Department Risk and Safety Psychology, University of Twente

Mod 12: BSc Thesis

Dr. N. M. A. Huijts

Dr. I. van Sintemaartensdijk

Date: 08.07.2024

Words: 8289

Abstract

This study explores the concept of informational privacy as a universal human value within Schwartz's theory of values, in a cross-cultural context. Informational privacy can be understood as the control about the extent to which personal information is shared towards others (Burgoon 1982). Through a questionnaire this study examines informational privacy among German and Romanian participants, the scope is expanded by also assessing convergent, predictive, and discriminant validity. In general, it can be said that the scale was partially validated. Findings showed a positive correlation between the human value "self-direction thought" and informational privacy, confirming conceptual similarities and convergent validity. Information privacy also has an effect on privacy protective behaviours such as managing location data settings on mobile devices, this was used to show predictive validity. No significant gender differences were found, however German participants displayed a higher score on informational privacy when compared to Romanians, this relates to discriminate validity. This study supports the definition of privacy as a multidimensional concept. Results indicate that informational privacy can be reliably measured as a distinctive dimension of privacy.

1. Introduction

A data breach is an event in which the data security of a large network or institution is compromised through a breach in confidentiality, posing a threat to the users' rights and freedoms. In 2015 the electronics company Vtech, a Hong Kong-based company that produces digital learning products and mobile devices aimed at young people was hacked, exposing the data of 6.4 million children (Miller, 2016). It was later stated by experts that Vtech failed to enact even the most basic of security measures that had been practice in the industry by that time for at least a decade, failing in properly securing their customers data by for example storing it in unencrypted plain text (Hunt, 2015).

This incident extends beyond a mere infringement on data security, it clearly demonstrates what can happen if personal information is centralised to such an extent and then treated carelessly. Furthermore, it prompts us to contemplate the consequences of our modern lifestyle, connecting appliances and everyday-objects around us. In cases such as the V-tech scandal one might say it is only about toys, however it is also about the fact that such a harmless object as a toy in our modern society can now pose a significant risk to our privacy. Therefore, it is important to critically examine the role of privacy in our modern society and how privacy fits into existing frameworks and scales.

2. Theoretical Background

2.1. Definitions of Privacy

Research regarding privacy has steadily gained more and more attention across many different fields, however agreement over a general definition or theory of privacy is still lacking. There are some studies, which are especially significant when it comes to their impact on the field. One example are the theories proposed by Alan Westin in his book "Privacy and freedom" in which he states that privacy can be defined as: "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1967, p.24). He describes privacy as an act of protection by the individual, through limiting access to others. One of his core ideas is a balance in the desire of privacy and disclosure. Westin says that the participation in society is an equally powerful desire and therefore these two forces regulate each other in a personal adjustment process. Therefore, Westin saw the nature of privacy as a resource of which you need a balanced amount that is just sufficient, otherwise unpleasant feelings arise.

Another important definition of privacy came from the researcher Altman (1975), who defined privacy as "the selective control of access to the self" (p.24). Altman saw privacy as especially important in the context of social and cultural interactions, he implies that privacy is always a part of society but is influenced by the culture in its expression. He also states that this definition of privacy does not only apply at a singular individual level, instead it also applies to groups. Similar to Westin, Altman agrees that privacy requires boundary control based on external influences and yourself. Altman distinguishes two levels of privacy, the actual and the desired level. When the actual and desired level of privacy are not equal it leads to negative emotions regarding your current level of perceived privacy. Therefore, it can be said that both Westin and Altman agree in their understanding of privacy as a resource with desired levels that have to be managed by oneself in relation to others.

2.2. Privacy Domains

Next to possible definitions of privacy as a resource, researchers found that privacy could be divided into multiple dimensions to arrive at a clearer picture. Theories proposed by Westin (1967) found four domains that he assumed to make up the elusive concept of privacy. He settled on the four domains called, intimacy, anonymity, solitude and reserve. According to him, solitude relates to personal space and not being observed, Intimacy is about the connections with people, anonymity is about the right to a private identity and lastly reserve is about the amount of information you share with others.

In 1982 Burgoon defined four related dimensions, psychological, social, physical and informational privacy. Within his framework, the domain of Informational privacy was defined by Burgoon as control over the acquisition and sharing of personal information. The domain of physical privacy referred to the level of physical separation between individuals. Controlling cognitive and affective inputs and outputs, such as values and beliefs belongs to the domain of psychological privacy Lastly, he defined the domain of social privacy as control about relationships and interactions with others.

These two theories about dimensions of privacy by Burgoon (1982) and Westin (1967) share some overlap with each other, while at the same time differing in other aspects. For example, when comparing Westin’s domain of anonymity and Burgoon’s domain of physical privacy, these two concepts share similarities in the fact that both focus on physical restriction from others. However, when comparing Westin’s domain of anonymity and Burgoon’s domain of social privacy, differences can be seen, with the former focussing on the aspect of identity and the latter focussing social interaction. These examples of research in the past show that privacy has been a complex concept and that there was no certain answer to the question what privacy is.

Just recently a study in the UK by Markink (2024) decided to take up the matter once more. She was among the first to consider measuring privacy as a value within an established framework called the Schwartz Theory of Values. Through a questionnaire she was able to identify three relevant domains of privacy, called informational privacy, observational privacy and social privacy. Additionally, her research also focussed on privacy related decision making when using social media. Her results indicated that only the dimension of informational privacy had significant correlations with the items measuring privacy decisions. Markink demonstrated that in the context of online communication via social media, the two domains social and observational privacy did not seem to influence the privacy decisions we make. Therefore, when deciding which one of the three domains defined by Markink is the most influential in this digital context, informational privacy stands out.

2.3. Informational Privacy

It is important to mention that an idea of informational privacy already existed before the digitalisation, however it is also clear that the term has gained new meaning and significance due to the abundance of digital information nowadays. Digital products are no doubt valuable tools in many ways. However, it is a fact that this privilege often comes with certain costs towards our informational privacy online. While online information has many upsides, there are some issues with the system in its current form. For example, users might find it harder to control not only what information is collected but also who will interact with it. Recently researchers started to pay closer attention to the concept of informational privacy. It has often been defined as the control about the extent to which personal information is shared towards others (Burgoon 1982). Another definition of informational privacy is the: “interest of individuals in exercising control over access to information about themselves” (van den Hoven et al., 2020, p.1).

The paper of Floridi (2005) introduced a different way of understanding informational privacy and its significance in modern society. He states that digital information and communication technologies (ICT’s) significantly changed the nature of the Infosphere, the space where information exists. Digital ICT’s, according to Floridi, not only possess the power to threaten or protect informational privacy, most importantly they also alter our perspective and beliefs on privacy as a whole. This perspective change brought about by digital ICT’s leads him to suggest that, in modern society personal information has become a significant part of what constitutes a person’s identity. Therefore, Floridi goes as far as to state that a breach of one’s informational privacy is equal to an act of aggression to one’s personal identity.

Informational privacy is especially important to study further, due to a phenomenon that is called the privacy paradox. The privacy paradox states that online privacy behaviours have been shown to be inconsistent with privacy attitudes. This means that even though people say that they are worried about their data they still tend to disclose personal information far beyond what would be consistent with their attitudes (Barnes, 2006). The existence of this inconsistency in privacy attitudes and behaviours points to a possible research gap in online privacy research. The insights of Floridi on how digital ICT’s reshaped our understanding of privacy, combined with the lack of consistency demonstrated in the privacy paradox, underscores how multifaceted and dynamic research on informational privacy is. It also highlights a need to try to reinterpret the current ways of how privacy behaviours and attitudes are measured, especially for informational privacy.

2.4. Privacy as a Value

Human values have the ability to steer opinions, attitudes and even behaviour, fundamentally shaping your personality and who you identify as. Many aspects of a person can be explained by looking at their values. Personality, opinions, behaviour and attitudes are all influenced and therefore can be predicted by measuring human values. Frameworks such as the Schwartz value theory strife to explain how values impact individual behaviour. Schwartz (1994) researched the relationship between values and behavioural patterns, with the goal to formulate what he called universal values. The ten values that he arrived at can be seen as guiding principles that aim to describe “desirable trans situational goals”. This means that these values can be considered as objectives people strive towards, which are relevant across many different contexts and situations. The aim of Schwartz’s research on this topic is to create a robust foundation to understand and predict human behaviour. Continuing this trend later he expanded this list to 19 human values (Schwartz, 2012), this was done to increase predictive power.

Recent research has raised questions concerning what actually predicts attitudes and behaviour towards informational privacy? Additionally, could informational privacy be considered a value in and of itself? Privacy as a concrete value has been measured in initial attempts and early studies, mainly by Huijts and Haans (2023) Markink (2024) and Jansen (2023). The currently most commonly used value measurement in psychology, Schwartz's theory of basic values does not include privacy as of yet (Schwartz et al., 2017). However, it has been shown that privacy could be a valuable addition to this list (Huijts & Haans, 2023; Jansen, 2023; Markink, 2024). Huijts and Haans (2023) argued for including privacy as a value within the theory because it fulfils some of the criteria, which are: "1. Values are concepts or beliefs, 2. They pertain to desirable end states, 3. Transcend specific situations, 4. guide selection or evaluation of behaviour and events, and 5. are ordered by relative importance." (Schwartz, 1992, p.4). Huijts and Haans research was done by adding information privacy items to the PVQ-RR standardised questionnaire. Through a confirmatory factor analysis, it was shown that information privacy was distinguishable from the rest of the values.

Furthermore, a multidimensional scaling analysis was used by Huijts and Haans (2023) and later by Markink (2024) to investigate the positioning of the privacy dimensions in a multidimensional scaling plot. In both instances a similar result was found, observational and social privacy were distinct from their neighbouring values. Both were found within the higher-order values quadrant, positioned around the same distance from the centre as the other 19 basic values. The third domain of Informational privacy however, was positioned within the middle of the motivational continuum, which is unusual. In his research Schwartz (2012) explained that, values closer to the centre are less abstract and more relevant in daily interaction. Additionally, values positioned closed to another tend to share underlying motivations. Informational privacy does not have a close neighbouring value, which indicates that this domain does not share underlying motivations with the other 19 basic values. Markink (2024) explains that the three items to measure informational privacy were based on social media use, a behaviour which is not particularly abstract and nowadays very relevant in daily interactions. These findings are in line with the theories of Schwartz, that more common values are more centred within the multidimensional scaling plot. Markink sees the unique positioning of the informational privacy domain as an interesting reason to further investigate whether this domain should be considered as a value placed in the middle of the continuum.

2.5. Research Aims and Questions

Markinks (2024) finding provided great insights into the dimensions of privacy and how they relate to decision making online, however she only conducted her study with participants living in the UK which leaves us with questions about the generalisability of her findings towards other cultures and countries. Her aim of including informational privacy as a new value within the established framework of Schwartz, benefits existing and future research by providing a more nuanced understanding of now privacy can be measured. This leads to more informed predictions regarding behavioural patterns of people in the digital context, thereby leading to more precise and effective development of policies. Further research is needed, to determine whether the three dimensions of privacy identified by Markink (2024) can be found in a different cultural setting. Therefore, it would make sense to apply her questionnaire to different population as well as extending the focus by checking for different types of validity. This paper will focus on the dimension of Informational privacy and it will be tested if informational privacy can be accurately measured, using Markinks (2024) questionnaire in a population of German and Romanian participants. To achieve this goal, in this study three types of validity are examined, which are convergent, predictive and discriminate validity.

Convergent Validity refers to the degree to which two measures, which are expected to be related based on theoretical expectations, are actually correlated. In other words, convergent validity is used to find out if your scale accurately captures what it is intended to measure, by inspecting relationships with conceptually associated concepts (Valkengoed et al., 2021). This type of validity is significant, because it provides evidence that the scale is measuring what it intends measure. Markink compared informational privacy to the all the established 19 values within Schwartz's framework and stated that information privacy had a positive correlation with only one, which was the value "self-direction thought" (Markink, 2024). Self-direction thought is explained as the "Freedom to cultivate one's own ideas and abilities" (Schwarzt, et al., 2012, p.669). Based on this formulation, there seems to be a conceptual similarity to placing high value on personal information. Furthermore, research by Dinev, Xu, Smith and Hart (2013) developed a framework for determining informational privacy and its correlates, with their aim being to clarify the often misunderstood concept. According to their findings, they were able to identify percieved information control and percieved risk as significant determinants of percieved informational privacy. Similar to Markinks (2024) research, these results underscore the idea that control over personal information, and therefore „self direction thought", is highly relevant to the perception of informational privacy. These findings support the notion, that individuals who particularly value informational privacy also seem to appreciate autonomy and freedom, to for example manage their private data. This correlation indicates that Markink indeed was able to demonstrate convergent validity in her sample from the UK. Therefore, in this study one aim is to test the scale by examining the relationship between informational privacy and self-direction thought, in a German and Romaninan sample.

Predictive validity is a criterion that shows how well a test can predict future outcomes (Valkengoed et al., 2021). It is a necessary as a characteristic of an accurate scale, demonstrating the practicality in real-world scenarios. To examine predictive validity, this study tests for the effect of informational privacy as a value on privacy protective behaviours. In the context of this study, this involves testing whether individuals who value informational privacy engage more often in privacy protective behaviour. Examples of such behaviours are actively restricting location data settings on your phone, dealing with cookie pop ups and the storage of personal sensitive documents. Research supports that these chosen behaviours can be indicators of privacy protective actions. A study by Paspatis et al. (2023) showed that individuals who place a high value on privacy tend to protect their personal information through various measures. These measures include for example configuring privacy settings and paying attention to data sharing agreements like cookies. Similarly, a study by Mühlhoff (2021) demonstrated that certain behavioural patterns are predictive of an persons concern for privacy. Behaviours such as managing the visibility of data and actively opting out of data sharing agreements, are according to him indicators of an high concern for privacy. The inclusion of items concerning privacy protective behaviours is a possible way to test the predictive validity of the scale. Therefore, the amount to which people value informational privacy is expected to correlate with their actual usage of privacy protective functions measured in this study.

Discriminate validity is used to find out if the measure is distinct and if it captures the specific concept it is supposed to measure without significant overlap into unrelated concepts. This is done by observing if scores show variances between groups where distinctions are anticipated based on previous theory (Valkengoed et al., 2021). The current study aims to specifically measure information privacy and how it differs between groups based on gender and nationality. In studies for example, that focussed on privacy as a whole, it has been shown that women tend to display higher scores in privacy concerns and behaviours than men (McGill & Thompson, 2021). The factor of Nationality seems to play an important role too. A study by Trepte and Masur (2016) explored national differences in attitudes towards privacy in social media, by comparing participants from the USA, UK, Germany, Netherlands and

China. The result was that western european nations such as the UK, Germany and Netherlands shared similar privacy perceptions and behavioural patterns. Participants from these countries generally had a smaller audience on social networks, tended to limit visibility of their posts and profile information more, and used more privacy settings. One finding was that especially German social media users seemed most concerned with such matters of online safety. These findings are in line with recent research into differences between nations on this matter, which also states that Germans value their privacy the most when compared to other nations (Prince & Wallsten, 2022). It is important to mention that a study directly comparing Germans and Romanians was not found, therefore it is not possible to give a completely accurate prediction on how these two would compare. However, the research by Masur (2016) clearly states that western european nations tend to be more concerned with matters of online safety. Therefore, it is likely that German participants are expected to score higher on informational privacy than the Romanian participants. In summary all three types of validity need to be tested to validate the scale developed by Markink (2024). This can be achieved through the following Research questions:

RQ1: Can informational privacy as a value be reliably measured in a population of German and Romanian participants?

RQ2: Is there a significant effect of informational privacy as a value on privacy-protective behaviors, such as managing location data settings on phones, handling cookie pop-ups, and storing personal sensitive documents?

RQ3: Is there a significant difference between men and women in informational privacy scores in a population of German and Romanian participants?

RQ4: Is there a significant difference between Romanian and German people in informational privacy as a value?

The following hypotheses relate to each research question:

H1: Informational privacy as a value has a positive correlation with the universal human value “self-direction thought”, showing convergent validity.

H2: Informational privacy as a value has a positive effect on privacy protective behaviour such as managing location data settings on phones, handling cookie pop-ups, and storing personal sensitive documents.

H3: Women score higher on Informational privacy as a value than men.

H4: Participants with German nationality score higher on Informational privacy as a value than Romanian participants.

3. Methods

3.1. Participants

The majority of the participants were found through snowball sampling carried out by the researchers. The second source of participants was the Sona system of the University of Twente which requires students to participate in studies for credit. In this case students of the UT who signed up via the Sona system received 0.25 credits for taking part. The requirements for being eligible to participate were a Dutch, German or Romanian nationality, however this paper focuses on the data of the German and Romanian participants primarily because only 5 Dutch participants finished the questionnaire. All participants filled out the survey in a language corresponding to their Nationality. Additionally, participants had to be over the age of 17 to take part.

In total n=230 German and Romanian citizens participated in this online survey study (164 Female, 66 Male, 0 Diverse, M_{age} = 34.7, *SD* = 15.8, range = 18 - 88 years). Of the participants 60% were German (137 total) and 40% were Romanian (93 total).

The first batch of Participants that was removed from the dataset was everyone who did the questionnaire in English. It was only 11 people, not a big enough sample to compare. In the German Questionnaire a total of 12 participants were removed, one due to the consent form and 11 due to attention checks. This resulted in 137 German participants remaining in the final data set. In the Romanian Questionnaire a total of 13 participants were removed from the analysis, three due to the consent form, 9 due to attention checks and one due to the age of the participant being younger than 18. This means 93 Romanian Participants were remaining. For the purpose of analysis, the method of Imputation was used, which replaces missing values with estimates based on the available data. Imputation was applied in total to 21 missing values during the first exploratory factor analysis that included all items found in Table 1. As long as more than 50% of the participants data was filled in, this method of dealing with missing values works well. This was the case in all analyses so no participants were excluded based on too many missing values.

3.2. Materials

The overall design of this study is an online survey study with closed questions only. The website Qualtrics was used to create and distribute the questionnaire as well as gather the responses. Participants would arrive at this website directly or via the Sona system of the UTwente. The following variables are measured:

3.2.1 Measurements

Schwartz 19 Values

The first part of the questionnaire is the so-called revised Portrait Values Questionnaire (PVQ-RR), which measures the 19 Values of Schwartz´s refined values theory through 57 items (Appendix 3). This standardized questionnaire was used in its original English form and the translated versions in German and Romanian (Schwartz, 2021). All of the items are formulated based on a fictional person with the same gender as the participant. It was decided to include both a female and a male version of the survey, this was done to increase the level of how much participants can relate to the statements. The statements were formulated based on the following schema. A fictional person states how important a specific situations or behaviour is to them and the participant has to identify how similar they are to the described fictional character in that aspect. A six-point response scale was used with a seventh "does not apply" option. (1) not like me at all, (2) not like me, (3) a little like me, (4) moderately like me, (5) like me, (6) very much like me, and (7) does not apply (Schwartz, 2017).

Table 1

Privacy Dimension items

Item No.	Items
	Informational Privacy:
2	It is important for him/her to be aware of what data is being collected about him/her while using the internet.
29	It is important for him/her to control what personal information is collected about him/her.
52	It is important for him/her to actively protect his/her online data.
	Social Privacy:
33	It is important for him/her to control how he/she interacts with others to meet his/her own needs.
48	It is important for him/her to have a space that is exclusively his/hers.
19	It is important for him/her to be able to control when he/she interacts with others close to him/her.
	Observational Privacy:
15	It's important to him/her that other people don't hear what he/she is discussing with her best friend.
41	It is important to him/her to control who can observe him/her in his/her home environment.
69	It is important for him/her to communicate with others without being overheard by others.

Privacy as a Value

Privacy as a value is measured using twelve additional items, three each for the four different kinds of privacy described in Markinks (2024) research: information privacy, observational privacy, social privacy, and solitude. These twelve additional items measure similarity like the rest of the PVQ-RR and can be answered using the same seven-point scale. Markink based these items on an exploratory factor analysis from the research of Jansen (2023). These twelve items were mixed with the PVQ-RR questionnaire to form the first part of the study which measures the different dimensions of privacy as a value within the Schwartz framework. Information privacy for example is measured with the item: „It is important to him/her to be aware of which data are collected about him/her while using the internet"

Privacy protective behaviour

The second part of the study is concerned with measuring privacy protective behaviour. This is achieved through 9 additional items formulated by the researchers of this study found in Table 2. To ensure that the formulations of the chosen behavioural items are not ambiguous a small pilot test was used to clear up any confusing aspects. Previous to that, a review of the existing literature on the topic was done. This had the aim of identifying what scales related to this topic are already validated and to see how researchers operationalised similar concepts before. Three out of the 9 items focus specifically on informational privacy behaviour, the remaining 6 are not that relevant for the current study, apart from the factor analysis in the beginning. The Items were formulated to measure similarity to a fictional person like the rest of the PVQ-RR and are answered using the same six-point scale. An example for an item measuring privacy protective behaviour in the context of informational privacy is: "In general, I actively select a narrower setting when I encounter cookie pop-ups (anything but "Accept all cookies")."

Additionally, two attention checks disguised as statements were included to ensure that participants were paying attention. One example for such an attention check would be the following item: "It is important that you pay attention to this study. To indicate that you have read this please tick: Not like me." In total this makes 57 PVQRR items, 12 Markink Items and two Attention checks, that together measure privacy as a value. For the second part there are 9 behavioural items measuring informational, social and observational privacy related behaviours.

Table 2

Privacy Behaviour items

Item No.	Items
	Informational Privacy:
70	In general, I check and manage the general location settings of my personal devices (e.g. Instagram Maps, TikTok).
73	In general, I actively select a narrower setting when I encounter cookie pop-ups (anything but "Accept all cookies").
76	In general, I tend to securely store sensitive personal documents (e.g. Important Receipts, Bank Statements, Medical Records) so that others cannot access them.
	Social Privacy:
71	In general, I prefer to solve personal problems myself instead of asking other people for help.
74	In general, I choose who I spend time with carefully.
77	In general, I try to limit my interactions with others to social events.
	Observational Privacy:
72	In general, I make sure I'm not noticed through my laptop camera, for example by covering the camera.
75	In general, I only have private conversations when no one else can hear them.
78	In general, I make sure that I am not observed while undressing or changing my clothes, for example by closing the curtains.

3.3. Procedure

Participants were told that the study is designed to measure how privacy is perceived and how it is connected to various privacy-related behaviours. They recieved this explanation and other details either in a Whatsapp message containing the link to participate or via the Sona System Website for Students. Informed consent was obtained though an online form participants had to fill in, before starting the questionaire (Appendix 2). In the consent form the methods for storing or sharing of the collected sensitive information was described, it was also highlighted that participation is voluntary and that it was possible to withdraw from the experiment. If participants would diagree with the consent form the study would end, if they would agree they were guided to the next section. After the consent form some demographic data was collected like the gender of the participant as well as the Nationality and Age. Based on this the participant recieved a male or female version of the questionaire for the rest of the study (Appendix 3). If the case occurred that a participant decided on “non-binary / third gender” or “prefer not to say” in the demographics a random version of the PVQ-RR questionnaire, male or female was be chosen. After completing the whole procedure participants were debriefed by a short written explaination and recieved the contact information of the researchers for further questions.

3.4. Data Analysis

The analysis was performed in R-studio and the script can be found in Appendix 6. To begin the analysis the data was transferred from Qualtrics to R-Studio. To clean up and prepare the dataset, participants that failed one of the two attention checks or had incomplete data for other reasons were to excluded from analysis. The answer option “does not apply” was first replaced by missing values. For the purpose of analysis, Imputation was used, which replaces missing values with estimates based on the available data.

The first step after cleaning the data-set, was to perform an exploratory factor analysis on the privacy dimension items to be able to find out if informational privacy items can be distinguished from the social and observational privacy items. Conducting an exploratory factor analysis first involves analysing the underlying factor structure through eigenvalues. Additionally, this method is supported by using a scree plot found in Appendix 1 and identifying the “elbow” point, which is the point on the scale after which the eigenvalues start to level off.

To answer the first research question, a Pearsons correlation test was used to measure the relationship between the factor determined to measure informational privacy as a value and “self-direction thought”.

A regression analysis was used to answer the second research question on if there is a significant effect of informational privacy as a value on privacy-protective behaviors. This analysis was done though first determining if the dependent variable privacy protective behaviour can be treated as a composite score or seperately. It was decided to treat it seperately and therefore three seperate regression analyses were performed, one for each of the behaviours. The independent variable informational privacy as a value was calculated through averaging the scores on the three dimension items number 2, 29 and 52.

To answer the third and fourth research question about the effect of gender and nationality on privacy as a value, two separate T-tests were performed. This way it was measured, if there is a significant difference between men and women as well as German and Romanian participants.

4. Results

4.1. Dimensions of Privacy as a Value

To determine if the chosen sample was factorable a Kaiser-Meyer Olkin measure was used, which suggested a good fit for a factor analysis (KMO=.71). This was also found with Bartlett's test of sphericity, which showed that the correlations are significant enough for this analysis (x^2=450.29, p<.001). These results indicate that the sample is indeed usable to proceed with a factor analysis.

At first an exploratory factor analysis using the varimax rotation method was used to reveal the factor structure. To measure the three different dimensions of privacy, nine items from the privacy scale were used. A three-factor model was chosen, due to fact that it was expected to represent the three dimensions of privacy with the highest accuracy. Furthermore, a scree plot, found in the Appendix under Figure 1, was used to visualise the eigenvalues, with the aim of further supporting the decision of using three factors. A clear elbow point was revealed after the second factor, suggesting that including the third factor adds meaningful variance. Therefore, the three-factor solution seems appropriate to represent the underlying dimensions. Further analysis showed that a three-factor model was able to explain 43.8% of the total variance in the sample. Item number 48, however had very weak loadings on all three factors, which meant removing it from the analysis might provide better results. A new factor analysis without including item 48 was tested and the resulting model had a better fit, explaining 46.7% of the total variance. The factor loadings derived from this approach can be found in Table 3, where the items are sorted into the respective dimensions of privacy. The results of the factor analysis including item 48 can be found in the Appendix as Table 5

Factor 1: Informational Privacy

Factor 1 includes the first 3 out of the 9 total items, 2, 29 and 52. This factor can be categorised as regarding everything related to online privacy and managing sensitive information. All three of the items belong to the privacy dimension of informational privacy with high factor loadings ranging from .75 to .78. The name of this factor is Informational privacy and it explains 20.5% of the total variance. This result suggests a straightforward conceptualisation of this factor representing what was measured as informational privacy. Therefore, for further analysis purposes information privacy as a value can be computed by averaging these items (M = 4.18, SD = 1.18, α = .82).

Factor 2: Social Privacy

Factor 2 includes the two items, which measure the domain of social privacy. This factor can be described as managing and keeping information secure from third parties during social interactions. The name of this factor is social privacy. The loadings of the two items contained within this Factor are .48 and .66 and explain 9.1% of the total variance. By averaging these two items the variable of social privacy as a value is calculated (M = 4.11, SD = 0.99, α = .51).

Factor 3: Observational privacy

Factor 3 includes three items, measuring observational privacy. The name of this factor is therefore Observational privacy. The loadings of the three items range from .52 to .61 and together explain 14.3% of the total variance. To conclude, by averaging these three items it is possible to calculate the variable of observational privacy as a value (M = 4.41, SD = 0.85, α = .39).

Table 3

Results of Exploratory Factor Analysis using three factors on Privacy as a Value Dimensions.

		Factor		
Item No.	Items	1	2	3
	Informational privacy:			
2	It is important for him/her to be aware of what data is being collected about him/her while using the internet.	**.76**	.01	.04
29	It is important for him/her to control what personal information is collected about him/her.	**.77**	.09	.12
52	It is important for him/her to actively protect his/her online data.	**.78**	.11	.02
	Social privacy:			
33	It is important for him/her to control how he/she interacts with others to meet his/her own needs.	.06	.05	**.66**
19	It is important for him/her to be able to control when he/she interacts with others close to him/her.	.04	.30	**.48**
	Observational privacy:			
15	It's important to him/her that other people don't hear what he/she is discussing with her best friend.	-.01	**.61**	.02
41	It is important to him/her to control who can observe him/her in his/her home environment.	.06	**.60**	.12
69	It is important for him/her to communicate with others without being overheard by others.	.17	**.52**	.23
	Eigenvalues	2.06	1.17	0.50
	% of Variance	55	31	13

After determining that the data set is factorable and reliable, the next step is to try and answer the first research question: "Can informational privacy as a value be reliably measured in a population of German and Romanian participants?" To answer this, the first hypothesis was tested, which stated: "Informational privacy as a value has a positive correlation with the universal human value "self-direction thought." A Pearsons correlation test was used to measure the relationship between Factor 1 determined to measure informational privacy as a value and "self-direction thought". The results demonstrated a significant positive correlation between the two variables (r = .23, t (229) = 3.65, p = <.001). The range of the 95% confidence interval for the correlation coefficient was between .10 and .35. The findings support the hypothesis that the universal human value “self-direction thought” is positively correlated with informational privacy as a value.

4.2. Privacy related Behaviours

Before beginning to test the second hypothesis regarding the behavioural items, it is necessary to first see if a similar factor structure can be found when compared to the Privacy dimensions items. A factor analysis including the nine behavioural items was used to see if similar factors can be found. Again, the Kaiser-Meyer Olkin measure was used, suggesting a good fit for a factor analysis (KMO=.70). Bartlett’s test of sphericity proved that the correlations are significant enough for this analysis (x^2=184.56, p<.001). These tests indicate that the behavioural items are suitable for a factor analysis. The output of the factor analysis on the privacy behaviour items can be found in Appendix Table 5. After conducting a factor analysis, with the three-factor model and comparing the results from the behavioural items to the factor structure found in the privacy dimension items, some differences can be seen. The underlying factor structure seems nothing alike with many split loadings and the little consistency within the contextual dimensions of informational, social and observational privacy. When taking a closer look at the three informational privacy related behaviour items, it becomes apparent that they should be treated as separate variables for the purpose of further analysis. This makes sense, due to the fact that all three measure different specific types of privacy protective behaviour related to informational privacy. Additionally, a low Cronbach’s alpha (0.54) implies a low level of internal consistency within these three items. To conclude, it is necessary to treat the behavioural items measuring informational privacy as separate variables, due to contextual factors and low internal consistency.

4.3.1 Predictive Validity:

A regression analysis examined the effect of one independent variable informational privacy as a value on the dependent variables, which are the three informational privacy related behaviours.

The results showed that informational privacy as a value has a statistically significant positive effect on managing general location settings on personal devices, $\beta = .354$, $SE = .067$, $t = 5.30$, $p < .001$.

Furthermore, the results also indicated that informational privacy as a value has a statistically significant positive effect on the behaviour of actively selecting narrower cookies settings $\beta = .210$, $SE = .080$, $t = 2.64$, $p = .009$.

Lastly the results showed a non-significant effect of informational privacy as a value on the behaviour of carefully storing personal documents like important receipts or bank statements $\beta = .122$, $SE = .070$, $t = 1.73$, $p = .085$

Based on this, the second hypothesis that Informational privacy as a value has a positive effect on privacy protective behaviour such as managing location data settings on phones, handling cookie pop-ups, and storing personal sensitive documents, can not be fully accepted. This is due to the fact that only two out of the three measured behaviours showed a significant effect.

4.3.2 Convergent Validity:

To arrive at a score representing what was supposed to measure the value self-direction thought, the answers on the corresponding three items, number 1, 28 and 47, were averaged. A correlation analysis between informational privacy as a value and the universal value self-direction thought revealed a significant positive correlation, $t(228) = 3.65$, $p < 0.001$, $R^2 = 0.06$. Based on, this the first hypothesis that Informational privacy as a value has a positive correlation with the universal human value self-direction thought, can be accepted

4.3.3 Discriminant Validity:

Gender Effects

To proceed with the third research question and to compare differences in men and women when measuring privacy as a value, a t-test was used. It was found that there are no significant differences between men and women in this population; t (228) = -0.45, p = 0.651, 95% CI [-0.418, 0.262]. This suggests that the third hypothesis „Women (M = 4.21) score higher on Informational privacy as a value than men (M = 4.13)." can not be accepted.

Nationality Effects

To answer the fourth research question and to compare privacy as a value between different Nationalities another T-test is used. It showed that there is a significant difference in information privacy scores when comparing German and Romanian participants, t (211) = 5.91, p = < .001, 95% CI = [0.573, 1.145]. These results support the fourth hypothesis that participants with German nationality (M = 4.70) score higher on informational privacy as a value than Romanian participants (M = 3.84).

5. Discussion

The aim of this study was to test whether informational privacy can be measured as a distinct dimension of privacy as a value in a population of Romanian and German participants. Additionally, the aim was also to validate the scale through looking at three different types of validity, predictive, convergent and discriminant validity. It was found that informational privacy is a distinguishable dimension of privacy within the population of German and Romanian participants. Furthermore, it was possible to partially validate the scale measuring informational privacy as a value.

5.1. Informational privacy as a Value Dimension

Based on prior research of Markink (2024), it was presumed that there are three different dimensions of privacy, called informational privacy, social privacy and observational privacy. According to the results described earlier, the first research question, "Can informational privacy as a value be reliably measured in a population of German and Romanian participants?" can be answered. It has been shown that informational privacy as a value can be measured as a distinct dimension in a population of German and Romanian participants. These results are in line with the findings of Markink (2024), who did her analysis in a UK population. This indicates that English Romanian and German people share a some understanding of what privacy is and how much they value it.

It is also necessary to consider cultural influences on privacy perceptions, such as the difference between individualistic and collectivistic cultures. Hofstede's (2011) cultural dimensions theory underscores this, by highlighting differences between individualistic cultures, such as the UK or Germany and collectivistic cultures such as for example Romania. The general rule is, that in individualistic societies personal privacy and especially autonomy is highly valued, where as in societies described as collectivistic, conformity and social harmony are prioritised (Hofstede 2011). This framework suggests that, even though informational privacy might be recognised universally as important, its emphasis on yourself or others might vary by a lot. Similar findings were reported by the researcher Li (2022). Their research also focussed on differences in privacy concerns in collectivistic and individualistic cultures. It was also observed that individualistic cultures are more protective of their privacy than collectivistic ones. This might explain why Romanian participants in this study showed a significantly lower score on information privacy as a value, when compared to German participants. The first research question can be answered as follows. Informational privacy as a value was reliably identified as a separate dimension in a German and Romanian population, as expected based on the results of Markink (2024).

5.2. Validity of Informational privacy as a Value

Predictive Validity

The results showed that predictive validity can be partially confirmed, because informational privacy as a value positively predicts privacy related behaviours such as restricting access of cookie messages and actively managing location data settings on personal devices. The behaviour of appropriately storing sensitive documents was not shown to be significantly impacted by information privacy as a value. This deviation might be due to the fact that the former two behaviours are could be interpreted as strictly online and the third behaviour is strictly offline. This observation suggests that there might be a difference in how German and Romanian treat privacy protective behaviours depending on if they are online or offline. To conclude it can be said that informational privacy has predictive power for some informational privacy related behaviours, especially for ones that are online. However, it could be tested more thoroughly, which leads to the conclusion that predictive validity is only partially met.

Convergent Validity

Convergent validity is met, due to the fact that informational privacy as a value is significantly correlated with the universal human value self-direction thought. It was argued that both concepts share conceptual similarities, such as autonomy and freedom (Schwartz et al., 2012). Based on, the findings it is concluded that support has been found for convergent validity.

Discriminant Validity

Demographic factors such as gender and nationality were included in this analysis with the goal in mind to test the discriminate validity of the scale. For the first part, the effect of gender, no significant differences were observed, which leads to rejecting the hypothesis that women tend to show a higher score on informational privacy. The results of this study can not full support the findings of McGill and Tompson (2021), that women tend to display higher scores in privacy concerns and behaviours than men. In their study they researched privacy as a whole and not informational privacy specifically, which might explain the difference. Another important point, which might explain these diverging results, is that there were 164 female and only 66 male participants. This might mean that males were underrepresented in this study when compared to females, which could lead to insufficient power to detect gender differences (Cohen, 1988). The effect of nationality, however displayed significant differences in the mean scores on privacy as a value. These results indicate that the hypothesis can be confirmed and german participants seem to have a higher value on information privacy. This outcome is in line with the findings of Trepte and Mansur (2016) and Prince and Wallsten (2022). To conclude, it can be said that discriminant validity was partially met in this research.

5.3. Limitations and Recommendations for Future research

The employed method of convenience sampling might be the reason why, even though the sample size was sufficient, not all types of validity were met. For future studies, it is reccomended to try to achieve a better balance in gender to have more accurate results. Researchers in future studies should consider adding additional predictors and specific contextual factors such as trust in technology or technological literacy. In the context of this study such factors are highly relevant and might predict the relationship between privacy values and behaviours. For example if users dont trust a platform it lowers the likelyhood of them sharing personal information. For technological literacy it is important that advanced users might be able to adapt their behaviour better to privacy risks. In other words, techologically literate users might use privacy settings more than the average person. Furthermore, future studies could benefit from adding cultural values and norms as a factor explicitly into the analysis. The two cultural dimensions of individualism and collectivism could help explain further how behaviours are shaped (Hofstede, 1984). Further exploring how these factors interact with informational privacy would help to broaden our understanding of cross culural differences in privacy attitudes. Lastly, another limitation is the cross sectional nature of the study, which limits is causal inferences. As a suggestion for further research, a longitudinal study in this topic might be interesting to examine measures like the stability of privacy values over time.

5.5. Conclusion

In conclusion this study underscores the significance of research in the domain of Privacy, especially when considering cultural contexts. This study shows that informational privacy can be measured as a distinct dimension in this population of German and Romanian participants. It also demonstrates that higher information privacy values can predict privacy-protective behaviour. There were no significant gender differences in the sample collected, but there were significant differences when it comes to nationality. Threats to privacy online and offline are constantly evolving. The findings of this study call attention to the need for culturally sentistive approaches when developing policies that protect us from bad actors.

References

Altman, I. (1975). The environment and social behaviour: privacy, personal space, territory, and crowding. Brooks/Cole Publishing Company

Barnes, S. B. (2006). A privacy paradox: Social Networking in the United States. *First Monday*. https://doi.org/10.5210/fm.v11i9.1394

Burgoon, J. K. (1982). Privacy and Communication. Annals of the International Communication Association, 6(1), 206–249. https://doi.org/10.1080/23808985.1982.11678499

Cohen, J. (1988). Statistical Power Analysis for the Behavioral Sciences (2nd ed.). Routledge. https://doi.org/10.4324/9780203771587

Dinev, T., Xu, H., Smith, J., & Hart, P.J. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. European Journal of Information Systems, 22, 295-316.

Floridi, L. (2005). The Ontological Interpretation of Informational Privacy. Ethics and Information Technology, 7, 185-200.

Hofstede, G. (2011). Dimensionalizing Cultures: The Hofstede Model in Context. *Online Readings in Psychology and Culture*, 2(1), 8-12. doi:10.9707/2307-0919.1014.

Huijts, N. M. A. & Haans, A. (2023). Values as causes of emotions towards a smart home device; extending the 19 values scale with privacy to understand emotions in digital contexts. Manuscript in preparation.

Hunt, T. (2015, November 28). *When children are breached – inside the massive VTech hack.* Troy Hunt. https://www.troyhunt.com/when-children-are-breached-inside/

Jansen, L.E. (2023). Privacy as a Value: Exploring the Integration of Privacy into Schwartz's Value Theory, Eindhoven University of Technology.

Li, Y. (2022). Cross-cultural privacy differences. Modern Socio-Technical perspectives on privacy, 267-292. https://doi.org/10.1007/978-3-030-82786-1_12

Markink (2024). Privacy as a Value, understanding conflicting values in the privacy paradox by using privacy as a distinctive value within Schwartz's value theory

McGill, T., & Thompson, N. (2021). Exploring potential gender differences in information security and privacy. *Information & Computer Security*, *29*(5), 850-865.

Miller, K. L. (2016). What we talk about when we talk about "reasonable cybersecurity": A Proactive and Adaptive Approach. *FLA. BJ*, *90*, 23-23.

Mühlhoff, R. Predictive privacy: towards an applied ethics of data analytics. *Ethics Inf Technol* **23**, 675–690 (2021). https://doi.org/10.1007/s10676-021-09606-x

Paspatis, I., Tsohou, A., & Kokolakis, S. (2023). How is privacy behavior formulated? A review of current research and synthesis of information privacy behavioral factors. *Multimodal Technologies and Interaction, 7*(8), 76. https://doi.org/10.3390/mti7080076

Prince, J. T., & Wallsten, S. (2022). How much is privacy worth around the world and across platforms?. *Journal of Economics & Management Strategy, 31(4)*, 841-861. https://doi.org/10.1111/jems.12481

Schwartz S. H. (1992). Universals in the content and structure of values: Theoretical advances and empirical tests in 20 countries. In Zanna M. P. (Ed.), *Advances in experimental social psychology, 25,* 1-65. San Diego, CA: Academic Press.

Schwartz, S. H. (2021). A Repository of Schwartz Value Scales with Instructions and an Introduction. *Online Readings in Psychology and Culture*, *2*(2). https://doi.org/10.9707/2307-0919.1173

Schwartz, S.H., Cieciuch, J., Vecchione, M., Davidov, E., Fischer, R., Beierlein, C., Ramos, A., Verkasalo, M., Lönnqvist, J., Demirutku, K., Dirilen-Gumus, O., & Konty, M. (2012). Refining the theory of basic individual values. *Journal of personality and social psychology, 103(4),* 663-688. https://doi.org/10.1037/A0029393

Schwartz, S. H., Cieciuch, J., Vecchione, M., Torres, C., Dirilen-Gumus, O., & Butenko, T. (2017). Value tradeoffs propel and inhibit behavior: Validating the 19 refined values in four countries. *European Journal of Social Psychology*, *47*(3), 241–258. https://doi.org/10.1002/ejsp.2228

Silverio-Fernández, M., Renukappa, S., & Suresh, S. (2018). What is a smart device? - a conceptualisation within the paradigm of the internet of things. *Visualization in Engineering*, *6*(1). https://doi.org/10.1186/s40327-018-0063-8

Trepte, S., & Masur, P.K. (2016). *Cultural differences in social media use, privacy, and self-disclosure : research report on a multicultural study.*

Van den Hoven, J., Blaauw, M., Pieters, W., Warnier, M. (2020). *Privacy and Information Technology, in: Zalta, E.N. (Ed.), Stanford Encyclopedia of Philosophy* (Summer 2020 Edition).

Van Valkengoed, A. M., Steg, L., & Perlaviciute, G. (2021). Development and validation of a climate change perceptions scale. *Journal of Environmental Psychology*, *76*. https://doi.org/10.1016/j.jenvp.2021.101652

Westin, A. F. (1967). Privacy and freedom. Washington and Lee Law Review, 25(1), 166

Appendix

Table 4

Results of Exploratory Factor Analysis including Item 48 on Privacy as a Value Dimensions.

		Factor		
Item No.	Items	1	2	3
	Informational privacy:			
2	It is important for him/her to be aware of what data is being collected about him/her while using the internet.	**.75**	.02	.05
29	It is important for him/her to control what personal information is collected about him/her.	**.76**	.10	.10
52	It is important for him/her to actively protect his/her online data.	**.78**	.13	.05
	Social privacy:			
33	It is important for him/her to control how he/she interacts with others to meet his/her own needs.	.06	.07	**.50**
48	It is important for him/her to have a space that is exclusively his/hers.	.17	**.36**	.18
19	It is important for him/her to be able to control when he/she interacts with others close to him/her.	.02	.26	**.63**
	Observational privacy:			
15	It's important to him/her that other people don't hear what he/she is discussing with her best friend.	-.04	**.74**	-.01
41	It is important to him/her to control who can observe him/her in his/her home environment.	.05	**.48**	.17
69	It is important for him/her to communicate with others without being overheard by others.	.16	**.50**	.28
	Eigenvalues	2.20	1.25	0.48
	% of Variance	55	31	12

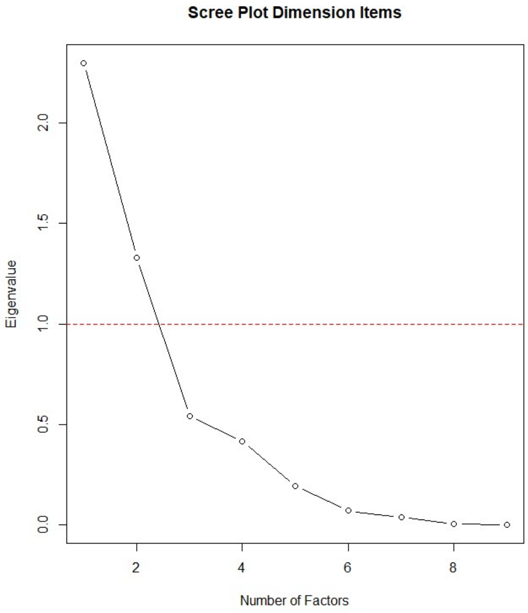
Table 5

Factor Loadings for Exploratory Factor Analysis of Privacy Behaviour items

		Factor		
Item No.	Items	1	2	3
	Informational privacy:			
70	In general, I check and manage the general location settings of my personal devices (e.g. Instagram Maps, TikTok).	**.70**	-.10	.19
73	In general, I actively select a narrower setting when I encounter cookie pop-ups (anything but "Accept all cookies").	**.58**	.31	-.10
76	In general, I tend to securely store sensitive personal documents (e.g. Important Receipts, Bank Statements, Medical Records) so that others cannot access them.	**.31**	.30	-.01
	Social privacy:			
71	In general, I prefer to solve personal problems myself instead of asking other people for help.	.01	.11	**.60**
74	In general, I choose who I spend time with carefully.	.15	**.39**	.28
77	In general, I try to limit my interactions with others to social events.	.01	**.44**	.13
	Observational privacy			
72	In general, I make sure I'm not noticed through my laptop camera, for example by covering the camera.	.31	**.35**	.02
75	In general, I only have private conversations when no one else can hear them.	.09	**.43**	.19
78	In general, I make sure that I am not observed while undressing or changing my clothes, for example by closing the curtains.	.06	**.36**	-.01
	Eigenvalues	1.57	0.64	0.41
	% of Variance	59	24	15

Figure 1

Scree plots for dimension items factor analyses



App.1

Informed consent:

Before you begin participating in this study, you are required to read about the procedures and other information you will encounter. At the end of this consent form, you will give your permission for using the collected data for research purposes.

● Purpose of the research
- The aim of this research is to measure how privacy is perceived and how it is connected to various privacy-related behaviours. This study is performed by Miruna Russa, Sophia Hochmann, and Matthias Giesen, students of the University of Twente, under the supervision of Nicole Huijts, who works at the same university.

● Risks of participating
- There are no risks associated with participation in this study. The research was reviewed and approved by the BMS Ethics Committee.

● Procedures for withdrawal from the study
- Your participation in this study is voluntary. In case you feel any discomfort while participating, you can withdraw from the study without giving any reasons and at any point during the participation. Your data will only be registered after reaching the end.

● Duration
- Completing this survey will take approximately 15 minutes.

● Personal Information
- In this study demographic data (gender, age, nationality) and experimental data (responses to the survey), will be collected, analyzed, and stored. The aim is to be able to answer the research questions and to possibly publish it in scientific literature.

- Usage of the data during and after research

- All the data will be treated with confidentiality and anonymously. The data will be locally stored on the computer of the researchers. The data collected in this study might also be of relevance for future research projects
- data will be stored on a private device under the regulations of the general data protection regulation (GDPR)
- Data will be stored for 10 years.

- Contact details of the researcher (or his/her representative)

m.russa@student.utwente.nl (for romanian participants)
m.j.giesen@student.utwente.nl
s.hochmann@student.utwente.nl
n.m.a.huijts@utwente.nl

If you have questions about your rights as a research participant, or wish to obtain information, ask questions, or discuss any concerns about this study with someone other than the researcher(s), please contact the Secretary of the Ethics Committee/domain Humanities & Social Sciences of the Faculty of Behavioural, Management and Social Sciences at the University of Twente by ethicscommittee-hss@utwente.nl

	Please tick the appropiate boxes	
	Yes (1)	No (2)
I have read and understood the study information and procedures. (1)	○	○
I consent voluntarily to be a participant in this study and understand that I can refuse to answer questions and I can withdraw from the study at any time, without having to give a reason. (2)	○	○
I understand that information I provide will be used only for research purposes, and it will be treated with confidentiality and anonymity. (3)	○	○
I give permission for the information and answers that I provide to be stored so it can be used for future research and learning. (5)	○	○

App. 2

Demographics Questions:

Q4 What is your gender?

○ Male (1)

○ Female (2)

○ Non-binary / third gender (3)

○ Prefer not to say (4)

Q5 What is your Nationality?

○ German (1)

○ Dutch (2)

○ Romanian (3)

Q6 What is your age in years?

App. 3

PVQRR example female version

Here we briefly describe different people. Please read each description and think about how much that person is, or is not like you. Put a checkmark in one of the boxes to the right of each question to indicate how much the person described is like you. How much like you is this person?

	Not like me at all (1)	Not like me (2)	A little like me (3)	Moderately like me (4)	Like me (5)	Very much like me (6)	Does not apply (7)
It is important to her to form her views independently. (1)	○	○	○	○	○	○	○
It is important to her to be aware of which data are collected about her while using the internet. (2)	○	○	○	○	○	○	○
It is important to her that her country is secure and stable. (3)	○	○	○	○	○	○	○
It is important to her to have a good time (4)	○	○	○	○	○	○	○
It is important to her to avoid upsetting other people. (5)	○	○	○	○	○	○	○
It is important to her that the week and vulnerable in society be protected. (6)	○	○	○	○	○	○	○
It is important to her that people do what she says they should. (7)	○	○	○	○	○	○	○
It is important to her never to think she deserves more than other people. (8)	○	○	○	○	○	○	○
It is important to her to care for nature. (9)	○	○	○	○	○	○	○

It is important that you pay attention to this study. To indicate that you have read this please tick "Not like me". (10)	○	○	○	○	○	○	○
It is important to her that no one should ever shame her. (11)	○	○	○	○	○	○	○
It is important to her to regulate the manner in which she interacts with others. (12)	○	○	○	○	○	○	○
It is important to her always to look for different things to do. (13)	○	○	○	○	○	○	○
It is important to her to take care of people she is close to. (14)	○	○	○	○	○	○	○
It is important to her to have the power that money can bring. (15)	○	○	○	○	○	○	○
It is important to her that others do not hear what she discusses with her best friend. (16)	○	○	○	○	○	○	○
It is very important to her to avoid disease and protect her health. (17)	○	○	○	○	○	○	○

It is important to her to be tolerant toward all kinds of people and groups. (18)	○	○	○	○	○	○	○
It is important to her never to violate rules or regulations. (19)	○	○	○	○	○	○	○
It is important to her to be able to control when she has interactions with others. (20)	○	○	○	○	○	○	○
It is important to her to make her own decisions about her life. (21)	○	○	○	○	○	○	○
It is important to her to have ambitions in life. (22)	○	○	○	○	○	○	○
It is important to her to maintain traditional values and ways of thinking. (23)	○	○	○	○	○	○	○
It is important to her that people she knows have full confidence in her. (24)	○	○	○	○	○	○	○
It is important to her to decide when to be by herself without any social interaction. (25)	○	○	○	○	○	○	○
It is important to her to be wealthy (26)	○	○	○	○	○	○	○

It is important to her to take part in activities to defend nature. (27)	○	○	○	○	○	○	○
It is important to her never to annoy anyone. (28)	○	○	○	○	○	○	○
It is important to her to develop her own opinions. (29)	○	○	○	○	○	○	○
It is important to her to control which personal information is collected about her. (30)	○	○	○	○	○	○	○
It is important to her to protect her public image. (31)	○	○	○	○	○	○	○
It is very important to her to help the people dear to her. (32)	○	○	○	○	○	○	○
It is important to her to be personally safe and secure. (33)	○	○	○	○	○	○	○
It is important to her to control how she interacts with others to meet her own needs. (34)	○	○	○	○	○	○	○
It is important to her to be a dependable and trustworthy friend. (35)	○	○	○	○	○	○	○

It is important to her to take risks that make life exciting. (36)	○	○	○	○	○	○	○
It is important to her to have the power to make other do what she wants. (37)	○	○	○	○	○	○	○
It is important to her to plan her activities independently. (38)	○	○	○	○	○	○	○
It is important to her to follow rules even when no-one is watching. (39)	○	○	○	○	○	○	○
It is important to her to be very successful. (40)	○	○	○	○	○	○	○
It is important to her to follow her family's customs or the customs of a religion. (41)	○	○	○	○	○	○	○
42 (42)	○	○	○	○	○	○	○
It is important to her to listen to and understand people who are different from her. (43)	○	○	○	○	○	○	○
It is important to her to have a strong state that can defend its citizens. (44)	○	○	○	○	○	○	○
It is important to her to enjoy life's pleasures. (45)	○	○	○	○	○	○	○

It is important to her that every person in the world has equal opportunities in life. (46)	○	○	○	○	○	○	○
It is important to her to be humble. (47)	○	○	○	○	○	○	○
It is important her to figure things out herself. (48)	○	○	○	○	○	○	○
It is important to her to honor the traditional practices of her culture. (49)	○	○	○	○	○	○	○
It is important to her to have a space that is exclusively hers. (50)	○	○	○	○	○	○	○
It is important to her to be the one who tells others what to do. (51)	○	○	○	○	○	○	○
It is important to her to obey all the laws. (52)	○	○	○	○	○	○	○
It is important to her to have all sorts of new experiences. (53)	○	○	○	○	○	○	○
It is important to her to actively protect her online data. (54)	○	○	○	○	○	○	○
It is important to her to own expensive things that show her wealth. (55)	○	○	○	○	○	○	○

It is important that you pay attention to this study. To indicate that you have read this please tick "Like me". (56)	○	○	○	○	○	○	○
It is important to her to protect the natural environment from destruction or pollution. (57)	○	○	○	○	○	○	○
It is important to her to take advantage of every opportunity to have fun. (58)	○	○	○	○	○	○	○
It is important to her to control who can be physically close to her. (59)	○	○	○	○	○	○	○
It is important to her to concern herself with every need of her dear ones. (60)	○	○	○	○	○	○	○
It is important to her that people recognize what she achieves. (61)	○	○	○	○	○	○	○
It is important to her never to be humiliated. (62)	○	○	○	○	○	○	○
It is important to her that her country protects itself against all threats. (63)	○	○	○	○	○	○	○

It is important to her never to make other people angry. (64)	○	○	○	○	○	○	○
It is important to her that everyone be treated justly, even people she doesn't know. (65)	○	○	○	○	○	○	○
It is important to her to avoid anything dangerous. (66)	○	○	○	○	○	○	○
It is important to her to be satisfied with what she has and not ask for more. (67)	○	○	○	○	○	○	○
It is important to her that all her firends and family can rely on her completely. (68)	○	○	○	○	○	○	○
It is important to her to be free to choose what she does by herself. (69)	○	○	○	○	○	○	○
It is important to her to accept people even when she disagrees with them. (70)	○	○	○	○	○	○	○
It is important to her to control who is able to see and hear her when she interacts with close others. (71)	○	○	○	○	○	○	○

App. 5
Behavioural Items female version

Here we briefly describe different behaviours. Please read each description and indicate how often or not often you engage in these behaviours. Put a checkmark in one of the boxes to the right of each question. How often do you engage in these behaviours?

	Never (1)	Rarely (2)	Regularly (3)	Often (4)	Always/Very often (5)	Does not apply (6)
I generally check and manage the location settings of my personal devices (e.g. Instagram, Maps, TikTok) (1)	○	○	○	○	○	○
I prefer to solve personal matters alone rather than asking people for help. (2)	○	○	○	○	○	○
I generally ensure that I am not observed through the camera of my laptop, for example by covering up the camera. (3)	○	○	○	○	○	○
I actively select a more restricted setting when encountering Cookies-Pop-ups (everything besides "Accept all cookies") (4)	○	○	○	○	○	○
I generally choose carefully with whom I spend time. (5)	○	○	○	○	○	○
I generally hold private conversations only when no one else can listen to them. (6)	○	○	○	○	○	○

I generally tend to keep sensitive personal documents (e.g. Important Receipts, Bank Statements, Medical records) in a designated location. (7)	○	○	○	○	○	○
I generally try to limit interactions with strangers at social events. (8)	○	○	○	○	○	○
I generally ensure that I am not observed while undressing or changing clothes, for example by closing the curtains. (9)	○	○	○	○	○	○

End of survey:

Thank you for participating in this study!

This research aims to measure three different dimensions of privacy (Informational privacy, social privacy, and observational privacy). Additionally it aims to include privacy as a value within the framework of universal human values proposed by Schwartz.

Study Contact Details for further Information:

m.russa@student.utwente.nl
m.j.giesen@student.utwente.nl
s.hochmann@student.utwente.nl
n.m.a.huijts@utwente.nl

App. 6

Script R-Code:

```
library(readxl)

library(dplyr)

library(psych)

library(car)

library(ltm)

COMBI_Data_Fin <- read_excel("COMBI Data Fin.xlsx")
COMBI_RDY_DATA <- subset(COMBI_Data_Fin, select = -c(InfCon1, InfCon2, InfCon3, InfCon4, ACheck1, ACheck2, Nationality))


# drop first row
COMBI_RDY_DATA <- COMBI_RDY_DATA[-1, , drop = FALSE]


for (col in names(COMBI_RDY_DATA)) {
  COMBI_RDY_DATA[[col]] <- as.numeric(COMBI_RDY_DATA[[col]])
}

# Define a function to replace 7 with NA
replace_7_with_NA <- function(x) {
  replace(x, x == 7, NA)
}

# Apply the function to variables Q1 to QB78
COMBI_RDY_DATA <- COMBI_RDY_DATA %>%
  mutate(across(Q1:QB78, replace_7_with_NA))
```

```
summary(COMBI_RDY_DATA)


# Demographics----------------------------------------------------------------------------------------

    # Compute mean, median, and other summary statistics for each group
    summary_stats <- COMBI_RDY_DATA %>%
      group_by(Language) %>%
      summarise(
        across(Gender:QB78, ~ mean(., na.rm = TRUE), .names = "mean_{.col}"),

        # Add other summary statistics as needed
      )

    summary(summary_stats)



    # Calculate the total number of female participants
    female_count <- sum(COMBI_RDY_DATA$Gender == "2", na.rm = TRUE)

    # Calculate the total number of male participants
    male_count <- sum(COMBI_RDY_DATA$Gender == "1", na.rm = TRUE)




    # Calculate mean age
    mean_age <- mean(COMBI_RDY_DATA$Age, na.rm = TRUE)

    # Calculate standard deviation of age
    sd_age <- sd(COMBI_RDY_DATA$Age, na.rm = TRUE)
    # Calculate the percentage of German participants
    # (Info Rom = 1, Ger = 2)
    german_percentage <- sum(COMBI_RDY_DATA$Language == "2", na.rm = TRUE) /
230 * 100

    # Calculate the total number of German participants
    german_total <- sum(COMBI_RDY_DATA$Language == "2", na.rm = TRUE)

    # Calculate the percentage of Romanian participants
    romanian_percentage <- sum(COMBI_RDY_DATA$Language == "1", na.rm = TRUE) /
230 * 100

    # Calculate the total number of Romanian participants
    romanian_total <- sum(COMBI_RDY_DATA$Language == "1", na.rm = TRUE)


# RQ1-------------------------------------------------------------------------------------------------------


  # Preparation for Factor analysis---------------------------------------------------------------------

   # Determine chosen sample and impute to remove missing values

    dimension_items <- COMBI_RDY_DATA[, c("Q2", "Q29", "Q52", "Q33", "Q48",
"Q19", "Q15", "Q41", "Q69")]    #!!!!!!!!! , "Q48" added now

   # Imputation
    dimension_items_imputed <- apply(dimension_items, 2, function(x) {ifelse(is.na(x),
mean(x, na.rm = TRUE), x)})
```

```
   # Amount of NAs in original data set  141
   original_na_count <- sum(is.na(COMBI_RDY_DATA))

   # Amount of Nas in relevant data set  21
   dimension_na_count <- sum(is.na(dimension_items))

   # Amount of NAs after Imputation 0
   imputed_dimension_na_count <- sum(is.na(dimension_items_imputed))



  # Determine if chosen sample of dimension items is usable for factor analysis

   # KMO
    kmo_result <- KMO(dimension_items)
    print(kmo_result)


   # Bartlett's test of sphericity

   # Check for constant columns
    constant_columns <- apply(dimension_items, 2, function(x) length(unique(x)) == 1)
    if (any(constant_columns)) {
     cat("The following columns are constant and will be removed:",
names(dimension_items)[constant_columns], "\n")
     dimension_items <- dimension_items[, !constant_columns]
    }

   # Ensure there are no missing values
    if (any(is.na(dimension_items))) {
     cat("Missing values found. Imputing missing values using mean imputation.\n")
     dimension_items <- apply(dimension_items, 2, function(x) ifelse(is.na(x), mean(x,
na.rm = TRUE), x))
```

```
    }

   # Calculate Bartlett's test of sphericity
    bartlett_result <- cortest.bartlett(cor(dimension_items), n = nrow(dimension_items))

   # Print the Bartlett's test result
    print(bartlett_result)



   # Cronbachs alpha
    alpha_result <- alpha(COMBI_RDY_DATA[, c("Q2", "Q29", "Q52", "Q33", "Q19",
"Q15", "Q41", "Q69")])    # !!!!!!! , "Q48" removed here now
    print(alpha_result)




  # Determine Number of Factors with Scree plot

    fa <- fa(dimension_items_imputed, nfactors = length(dimension_items[1,]), rotate =
"varimax")

   # Find eigenvalues and create a scree plot to find the elbow point
    eigenvalues <- fa$values

    plot(eigenvalues, type = "b", main = "Scree Plot Dimension Items", xlab = "Number of
Factors", ylab = "Eigenvalue")

    abline(h = 1, col = "red", lty = 2)




 # Dimension Items First Factor analysis with THREE Factor Model
```

```
    fa <- fa(dimension_items_imputed, nfactors = 3, rotate = "varimax", min.loadings = 0)


    print(fa$loadings, cut = 0)


   #Eigenvalues (care for 2 or 3 factors)

    # Extract eigenvalues
    eigenvalues <- fa$values

    # Print eigenvalues
    print(eigenvalues)

   #Percentage of Variance (care for 2 or 3 factors and if 48 or not)

    # Total sum of eigenvalues
    total_variance <- sum(eigenvalues)

    # Calculate the percentage of variance explained by each factor
    percentage_variance <- eigenvalues / total_variance * 100

    # Print the percentage of variance explained by each factor
    print(percentage_variance)




# Behavioral items factor analysis:
  behaviour_items <- COMBI_RDY_DATA[, c("QB70", "QB73", "QB76", "QB71", "QB74", "QB77", "QB72", "QB75", "QB78")]

  behaviour_items_imputed <- apply(behaviour_items, 2, function(x) {ifelse(is.na(x), mean(x, na.rm = TRUE), x)})

#KMO

  kmo_result <- KMO(behaviour_items)
  print(kmo_result)



#Bartlett's test of sphericity

  # Check for constant columns
  constant_columns <- apply(behaviour_items, 2, function(x) length(unique(x)) == 1)
  if (any(constant_columns)) {
    cat("The following columns are constant and will be removed:", names(behaviour_items)[constant_columns], "\n")
    behaviour_items <- behaviour_items[, !constant_columns]
  }

  # Ensure there are no missing values
  if (any(is.na(behaviour_items))) {
    cat("Missing values found. Imputing missing values using mean imputation.\n")
    behaviour_items <- apply(behaviour_items, 2, function(x) ifelse(is.na(x), mean(x, na.rm = TRUE), x))
  }

  # Calculate Bartlett's test of sphericity
  bartlett_result <- cortest.bartlett(cor(behaviour_items), n = nrow(behaviour_items))
  # Print the Bartlett's test result
  print(bartlett_result)


#FA

  fa <- fa(behaviour_items_imputed, nfactors = 3, rotate = "varimax", min.loadings = 0)


  print(fa$loadings, cut = 0)


#Eigenvalues

  # Extract eigenvalues
  eigenvalues <- fa$values

  # Print eigenvalues
  print(eigenvalues)


#Percentage of Variance

  # Total sum of eigenvalues
  total_variance <- sum(eigenvalues)

  # Calculate the percentage of variance explained by each factor
  percentage_variance <- eigenvalues / total_variance * 100

  # Print the percentage of variance explained by each factor
  print(percentage_variance)


# Cronbachs alpha
```

```
    alpha_result <- alpha(COMBI_RDY_DATA[, c("QB70", "QB73", "QB76")])
    print(alpha_result)


# Dimension Items Second Factor analysis with TWO Factor Model

    fa <- fa(dimension_items_imputed, nfactors = 2, rotate = "varimax", min.loadings = 0)


    print(fa$loadings, cut = 0)


   # Eigenvalues (care for 2 or 3 factors)

    # Extract eigenvalues
    eigenvalues <- fa$values

    # Print eigenvalues
    print(eigenvalues)


   #Percentage of Variance (care for 2 or 3 factors)

    # Total sum of eigenvalues
    total_variance <- sum(eigenvalues)

    # Calculate the percentage of variance explained by each factor
    percentage_variance <- eigenvalues / total_variance * 100

    # Print the percentage of variance explained by each factor
    print(percentage_variance)
```

```
# Cronbachs alpha


   alpha_result <- alpha(COMBI_RDY_DATA[, c("Q2", "Q29", "Q52")])
   print(alpha_result)



# Correlation analysis--------------------------------------------------------------------------------


  # Factor analysis based on 3 factor model
   #fa_model <- fa(dimension_items_imputed, nfactors = 3, rotate = "varimax")

  # Extract loadings
   #loadings_matrix <- fa_model$loadings[, 1:2]

   # Compute factor scores manually
   #MR1_scores <- as.matrix(dimension_items_imputed[, c("Q2", "Q29", "Q52")]) %*% loadings_matrix[1:3, 1]


   information_privacy_scores <- rowMeans(COMBI_RDY_DATA[, c("Q2", "Q29", "Q52")], na.rm = TRUE)


  # Assuming your data is in a dataframe called COMBI_RDY_DATA
   self_direction_scores <- rowMeans(COMBI_RDY_DATA[, c("Q1", "Q28", "Q47")], na.rm = TRUE)


  # Correlation test
   #cor_test <- cor.test(MR1_scores, self_direction_scores)
```

```
     cor_test <- cor.test(information_privacy_scores, self_direction_scores)

    print(cor_test)



# RQ2---------------------------------------------------------------------------------------------------


  # Step 0: Find out of Dependent variable should be treated as a composite score or
separately, by looking at reliability

    alpha_result <- alpha(COMBI_RDY_DATA[, c("QB70", "QB73", "QB76")])
    print(alpha_result)


  # Step 1: Define dependent variables (privacy-protective behaviors)
    three_privacy_behaviors <- COMBI_RDY_DATA[, c("QB70", "QB73", "QB76")]

    location_behaviour <- COMBI_RDY_DATA[, c("QB70")]
    popup_behaviour <- COMBI_RDY_DATA[, c("QB73")]
    document_behaviour <- COMBI_RDY_DATA[, c("QB76")]



  # Step 2: Calculate the information privacy score
    COMBI_RDY_DATA$InfoPrivacyScore <- rowMeans(COMBI_RDY_DATA[, c("Q2",
"Q29", "Q52")], na.rm = TRUE)

  # Step 3: Create a new data frame with the necessary variables
    regression_data <- COMBI_RDY_DATA %>%
      select(InfoPrivacyScore, QB70, QB73, QB76)

    regression_data <- COMBI_RDY_DATA %>%
      dplyr::select(InfoPrivacyScore, QB70, QB73, QB76)

  # Step 4: Run the regression analysis
    # We need to reshape the data for a multiple linear regression, considering the dependent variables collectively
    # Since we have multiple dependent variables, we will run three separate regressions

    model_QB70 <- lm(QB70 ~ InfoPrivacyScore, data = regression_data)
    model_QB73 <- lm(QB73 ~ InfoPrivacyScore, data = regression_data)
    model_QB76 <- lm(QB76 ~ InfoPrivacyScore, data = regression_data)

  # Step 5: Summarize the results
    summary(model_QB70)
    summary(model_QB73)
    summary(model_QB76)

  # Print the coefficients to see the effects
    cat("Effect of InfoPrivacyScore on QB70:\n")
    print(coef(model_QB70))
    cat("Effect of InfoPrivacyScore on QB73:\n")
    print(coef(model_QB73))
    cat("Effect of InfoPrivacyScore on QB76:\n")
    print(coef(model_QB76))




# RQ3----------------------------------------------------------------------------------------------------


    # Ensure Gender is a factor
    COMBI_RDY_DATA$Gender <- as.factor(COMBI_RDY_DATA$Gender)
```

```
# Information privacy score is the mean of Q2, Q29, and Q52
COMBI_RDY_DATA$InfoPrivacyScore <- rowMeans(COMBI_RDY_DATA[, c("Q2", "Q29", "Q52")], na.rm = TRUE)

# Check normality (info M = 1, F = 2)
shapiro_male <- shapiro.test(COMBI_RDY_DATA$InfoPrivacyScore[COMBI_RDY_DATA$Gender == "1"])
shapiro_female <- shapiro.test(COMBI_RDY_DATA$InfoPrivacyScore[COMBI_RDY_DATA$Gender == "2"])

print(shapiro_male)
print(shapiro_female)

# Check for equal variances
levene_test <- leveneTest(InfoPrivacyScore ~ Gender, data = COMBI_RDY_DATA)
print(levene_test)

# Determine if variances are equal
var_equal <- levene_test$`Pr(>F)`[1] > 0.05



# Perform t-test
t_test_result <- t.test(InfoPrivacyScore ~ Gender, data = COMBI_RDY_DATA, var.equal = var_equal)
print(t_test_result)



# Alternative: Perform Mann-Whitney U test due to non-normality
wilcox_test_result <- wilcox.test(InfoPrivacyScore ~ Gender, data = COMBI_RDY_DATA)
print(wilcox_test_result)
```

```
# RQ4------------------------------------------------------------------------------------------------------------------------------------------------------------------

    # Ensure Language (Nationality) is a factor
    COMBI_RDY_DATA$Language <- as.factor(COMBI_RDY_DATA$Language)

    # Information privacy score is the mean of Q2, Q29, and Q52
    COMBI_RDY_DATA$InfoPrivacyScore <- rowMeans(COMBI_RDY_DATA[, c("Q2", "Q29", "Q52")], na.rm = TRUE)

    # Check normality for each group
    shapiro_german <- shapiro.test(COMBI_RDY_DATA$InfoPrivacyScore[COMBI_RDY_DATA$Language == "2"])
    shapiro_romanian <- shapiro.test(COMBI_RDY_DATA$InfoPrivacyScore[COMBI_RDY_DATA$Language == "1"])

    print(shapiro_german)
    print(shapiro_romanian)

    # Perform t-test
    t_test_result_language <- t.test(InfoPrivacyScore ~ Language, data = COMBI_RDY_DATA)
    print(t_test_result_language)

# END------------------------------------------------------------------------------------------------------------------------
```