Revisiting Privacy Scales: An Investigation into the Ability of Privacy Scales to Capture & Distinguish Granular Privacy Constructs

HABIBA FARZAND, University of Bristol, UK and University of Glasgow, UK
SARAH ABDELWAHAB GABALLAH, Ruhr University Bochum, Germany
SHAUN MACDONALD, University of Glasgow, UK
MOHAMED KHAMIS, University of Glasgow, UK
KAROLA MARKY, Ruhr University Bochum, Germany

Abstract

Purpose: Privacy scales are scientific instruments to measure user attitudes, perspectives, preferences, and concerns. However, their ability to reliably capture underlying constructs depends on the individual's interpretation of the scales' statements. Recent work by Colnago et al. [7] investigated the users' understanding of statements of commonly used privacy scales with a US-based sample. They found significant misalignments between what the constructs aim to measure and the users' understanding.

Methodology: In this paper, we reproduced the work by Colnago et al. by targeting a representative from the UK (N=390) instead of the US. We distributed an online survey and asked participants about their understanding of commonly used privacy constructs such as behaviour, perception, and the like.

Findings: Our results provided evidence that no statement uniquely measured only one construct, and the misalignment of scale constructs and users' understanding exists between the US and the UK. The misalignment indicates that, regardless of the commonality of the primary language of both countries, scale statements are perceived as measuring different constructs by both populations.

Research Limitations: Like all online surveys, our results might suffer from response biases, such as wrong self-assessments. Furthermore, since online questionnaires do not involve interaction with an examiner, participants might have misinterpreted the sentiment behind a question. However, our study and the original study by Colnago et al. aimed to investigate precisely that.

Practical Implications: Our findings highlight the need to revisit construct definitions and conduct cross-cultural scale validation studies. We discuss the possible underlying reasons and best practices for future scale development studies. We publicly make our data collection and analysis code available to allow for replication and further investigations.

Keywords: Privacy Scales, Usable Privacy, Measurement Scales

1 INTRODUCTION

Privacy is a highly individual concept because privacy preferences differ among individuals [37]. Different privacy scales have been proposed to capture these individual differences in various contexts, such as IUIPC [27], or the SA-6 for assessing security attitudes [9].Privacy scales are vital for providing insights into public opinions and user perspectives, guiding the design of privacy-enhancing technologies and policies. Therefore, it is essential that scales precisely measure the desired constructs, also defined as scale validity [5, 8]. The absence of (optimum) scale validity leads to inaccurate measurements, which lack predictive power and cannot be used to generalize results [38]. A crucial aspect of scale

Authors' Contact Information: Habiba Farzand, habiba.farzand@bristol.ac.uk, University of Bristol, UK and University of Glasgow, UK; Sarah Abdelwahab Gaballah, Ruhr University Bochum, Germany; Shaun Macdonald, University of Glasgow, UK; Mohamed Khamis, University of Glasgow, UK; Karola Marky, Ruhr University Bochum, Germany.

© 2025

validity assessment is the target audience's unambiguous understanding of statements, as accurate understanding ensures accurate measurement.

In 2022, Colnago et al. [7] were the first to explore how well target audiences understand statements of four common privacy scales. For this, they analysed the interpretation of statements of (1) IUIPC [27], (2) CFIP [35], (3) GIPC [27], and (4) Westin's Privacy Segmentation Index [37]. They also tested a set of items generated by experts to verify if the item statements represented the construct they aimed to measure. The scale and generated statements were matched against six constructs: (1) privacy attitude, (2) privacy preference, (3) privacy concern, (4) privacy expectation, (5) privacy decision, and (6) privacy behaviour with a US representative sample (N=400).

The study of Colnago et al. [7] provided evidence of the mismatch between the expected and aimed constructs of the scales, indicating a lack of validity. For example, the study participants perceived a construct aimed at measuring privacy concerns as measuring privacy preferences. Further, Colnago et al. [7] also reported that no statement uniquely measured any construct. Overall, their results showed that most of the investigated statements measured more than one construct.

This paper continues the line of research started by Colnago et al. by replicating and extending their work around the understanding of scale statements, specifically investigating the following research questions:

RQ1: How do UK citizens interpret statements of common privacy scales?

RQ2: To what extent are statements of common privacy scales interpreted differently by US and UK citizens?

We conducted a statement classification study with a representative sample (N=390) from the UK. We asked the participants to rate the 70[1] statements from the original study concerning the six constructs. We used the same definitions of each construct as the original study to ensure methodology consistency.

On the one hand, we found that similar to US users, the UK users' interpretation of the statements differs from the construct the statement aims to measure. The differences in interpretation varied for each scale. For example, with respect to Westin's Privacy Segmentation, only one statement measured the expected construct. On the contrary, almost all statements in the CFIP scale measured the expected construct. Whereas among the generated items, the majority of the statements were not associated with their expected construct. On the other hand, while our results partly confirm results from Colnago et al., we overall found more differences in interpretation among UK users compared to the US sample, most prominently among the generated statements. The results showed that privacy `concern` was the most allocated construct in the US and the UK sample. Moreover, privacy `behaviour` and `decision` classifications were more prominent in the US than in the UK. Privacy `expectation` and `preference` were more highlighted in the US than in the UK sample.

We conclude with a holistic view of the results, including the original study and the replication study, showing a lack of congruence between what each construct aims to measure and what it is observed to be measuring. Since different results were observed in the US and the UK, this motivates frequent investigations of (1) construct definitions, (2) linguistic accuracy, and (3) cross-cultural evaluations of scale questionnaires. This is important to ensure scale validity over time and over cultures. This paper makes the following contributions:

(1) **Investigation of Understanding of Scale Statements:** We replicate and extend the findings about the users' understanding of four common privacy scales from Colnago et al. [7] with a representative sample from the UK (N=390). We provide evidence of a significant misalignment between what each construct is expected to

[1]While the original paper mentions a total of 69 statements, adding up the number of statements results in 70 instead of 69 statements.

measure and what it is observed to be measuring. While we partly confirm the results from Colnago et al., we also provide new insights from our UK sample and compare both populations.

(2) **Recommendations for Scale Development & Validation Studies:** Our results show significant differences between the US and UK samples, even though they share one native language. Based on the original study and related work, we present recommendations and lessons learned for scale development and validation.

(3) **Replication Package:** We make our data collected and analysis code publicly available at Zenodo [13] to allow for replication and further investigations of other communities, such as speakers of other languages or non-WEIRD communities.

The remainder of the paper is structured as follows: Section 2 presents background information on cross-cultural privacy investigations and various privacy scales developed for use for multiple purposes. Section 3 presents the methodology followed in this paper and section 4 presents the results. Finally, section 5 discusses the results, provides recommendations for scale development, and presents future research directions.

2 BACKGROUND & RELATED WORK

This section overviews cross-cultural privacy investigations and provides background information on privacy scales.

2.1 Privacy Studies Across Multiple Countries

As we move across different countries, differences exist in how technology is used and perceived. Different types of studies investigated different subsets of countries.

Herbert et al. [19] conducted a large-scale study with 12.000 participants from around the world, showing that the country of residence can be used as a predictor for privacy concerns. In this context, the amount of privacy and security misconceptions among UK and US residents was largely similar. Trepte et al. examined the privacy calculus, i.e., an individual's willingness to share information online in exchange for a benefit, in five countries (US, UK, Germany, Netherlands, and China) [36]. They underpin the impact of cultural background on privacy aspects. As also shown by other related work [23, 33, 22], the axis of individualism-collectivism played an important role. Li et al. [26] used different axes (like individualism-collectivism) to predict privacy decisions, again confirming these differences.

Further studies investigated narrower scopes. The use of social media is seen as a way of communication and connection more commonly by users in China and Korea (i.e. collectivist countries) compared to users in the US [22]. Further, differences in perceptions of information disclosure between German and US users were reported [23]. US users, in particular, were found to have more privacy concerns than German users [23]. Similarly, shoulder surfing - observing someone's device screen without permission [11], is perceived differently in different cultures and is reported to have more severe consequences in the Arab world in comparison to Germany [33]. Along the same lines, differences were also demonstrated by related work on an even smaller scale than the overall societies. Culturally shared privacy norms were found to even differ within one country. Studies in the US revealed differences in the usage of privacy settings among White Americans and Asian Americans, African Americans, and Hispanic Americans [17].

This paper investigates differences between the US and the UK. Data collection and use are regulated differently in the two countries [16]. Services in the UK have to adhere to the GDPR, while there are primarily domain-specific privacy regulations in the US. Privacy is also perceived differently by the general public in the US and the UK, as seen in multiple scenarios. Several studies already outlined above investigate the UK and the US in their samples, as well as other countries. Overall, it has been shown that the countries share individualism [36] yet behave differently in

narrower contexts, such as using banners where people in the UK are more likely to accept all cookies than those in the US [3].

To sum up, prior work provides evidence that views and perceptions of privacy change as we move across cultures globally, but differences could also be evident within one country. Based on this body of work, we investigate potential privacy perception differences in two countries that share the same – or at least extremely similar – native language: the US and the UK. We introduce more comparisons between those countries in the next section.

2.2 Investigated Privacy Scales

The differences in privacy have led to the need for the development of privacy scales to measure granular concepts, such as concerns or preferences. Privacy scales have been developed since 1967 when Alan Westin presented the *privacy index* [37] and as technology and knowledge have evolved, more and more privacy-related scales are being developed, for example, out-of-device privacy scale [10], the value of other people's privacy scale [18] and alike.

In this work, we investigate the four commonly used privacy scales: (1) Internet Users' Information Privacy Concern (IUIPC) [27], (2) Concern For Information Privacy (CFIP) [27], (3) Global Information Privacy Concern (GIPC) [35], and (4) Westin's Privacy Segmentation Index [20]. The IUIPC scale was developed by Malhotra et al. to capture users' privacy concerns regarding online information privacy [27]. The scale has ten items comprising three subscales: awareness, control, and collection. The IUIPC was adapted from CFIP and designed to measure privacy concerns. More specifically, the subscale "collection" was taken from CFIP. Recent work on scale validation has shown that an 8-item IUIPC offers better statistical support and outperforms the validity and reliability of a 10-item IUIPC scale [15]. However, Colnago [7] used the 10-item IUIPC scale, which is why we also use the 10-item version. CFIP [35] is a 15-item scale with four subscales that measure different dimensions of privacy concerns, including errors, unauthorized use, improper access and collection. The GIPC scale is also aimed at measuring privacy concerns and is composed of six statements.

All three scales mentioned – IUIPC, CFIP, and GIPC – use 7-point Likert items. In contrast to these scales, Westin's Privacy Segmentation Index presented privacy indexes to capture changes in privacy perspectives over time. To use Westin's Privacy Segmentation Index, the statements are presented on a 4-point scale and then based on the responses, participants are classified either as privacy fundamentalists, privacy unconcerned or privacy pragmatists. While these scales have been developed for various purposes, validation checks must occur periodically and in multiple contexts, for example, with a different population. This is necessary to ensure accurate measurement.

> **Summary:** As seen in prior work, differences in privacy norms and perceptions exist between different populations. To measure different dimensions of privacy, such as concern or preferences, researchers have proposed numerous scientific scales, for example, IUIPC by Malhotra et al. [27]. While such scales are an important contribution to the field of knowledge, their validation is an ongoing process. A significant form of validation is ensuring that different populations understand scale statements accurately.

3 METHODOLOGY

In this section, we describe our replication methodology. We opted for a replication study with a representative sample from the UK to investigate whether the findings generalize between the US and the UK. The US and the UK have English as the official language, but there are differences between vocabulary and dialects, which might impact how statements are understood. The understanding of statements reflects the extent to which participants associate each statement with each construct. Further, both countries vary in their cultural norms and values, which might impact how they

perceive various sub-categories of privacy, such as privacy expectations or concerns. Due to the above-listed reasons, we opted to investigate to what extent the findings from Colnago et al. [7] can be generalized to the UK population.

3.1 Achieving Replication

1) Study Design: We based our study design on the original study as detailed by Colnago et al. in their publication [7]. We also got in touch with the lead author to clarify any misunderstandings regarding the study design. Furthermore, we used the identical set of statements as in the original study, which consisted of 31 scale statements (IUIPC [27], GIPC [27], CFIP [35], and Westin's Privacy Segmentation Index [20] as described in Sec. 2) and 39 expert-generated statements, totalling 70 statements.

2) Study Procedure: The participants first read and accepted a consent form. Then, we instructed participants to rank each statement with respect to the six constructs, namely, privacy concern, attitude, preference, expectation, decision, and behaviour. We used the same construct definition set as the original study (see Table 2). For the list of the scale statements and the generated items, the reader is referred to Table 1 and 4. Similar to the original study, we presented participants with the prompt, "*Imagine that you are talking to a friend, and your friend says the following sentence:*", after which a randomly selected statement was shown to the participants. Then, they were asked to rate how well each of the constructs represented what was being said by their friend. Each statement was rated on a 5-point scale, ranging from *1 = "does not describe at all"* to *5 = "describes extremely well"*. Each participant was presented with a random selection of seven statements, and approximately 40 participants rated each statement. All participants were presented with all construct names and their respective definitions. To check for participants' attentiveness, we checked for completion time of the study. Participants who completed the study too quickly or too excessively long were excluded from the study.

3.2 Participant Demographics

We recruited a sample of N=390 participants from the UK via the Prolific online platform [32]. We opted for a representative sample of the UK - a tool available on Prolific that reflects the demographic distribution of the UK based on the statistics from the UK Office of National Statistics [29]. We selected a representative sample as it helps in making results generalisable. Out of N=390 participants, 51.5% participants identified as female and 48.5% as male. Participants were, on average, 46.27 years old (SD=15.95, min=18, max=104). When asked about ethnicity, 84.35% of the participants identified as White, 7.43% as Asian, 3.07% as Black, and 2.56% as mixed and other, respectively. Lastly, 17.17% of participants reported working or studying in a technology-related field.

3.3 Ethical Considerations

The study was approved by the IRB of our institution prior to execution. Participants were informed about the research study and what was expected before participation. They were further informed that they could abort the survey study at any time without fearing negative consequences. We obtained consent from each participant before the study. Finally, we reimbursed participants at an hourly rate of approximately nine pounds.

4 RESULTS

This section presents the results of statement interpretation by a representative sample based in the UK. The results are based on primary constructs and meta-constructs and are broken down by scale. In each section, we first describe

Scale		Statements
Westin's Privacy Segmentation Index		Consumers have lost all control over how personal information is collected and used by companies. Most businesses handle the personal information they collect about consumers in a proper and confidential way. Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today
GIPC		To me it is the most important thing to keep my privacy intact from online companies. Compared with other subjects on my mind, personal privacy is very important Compared to others, I am more sensitive about the way online companies handle my personal information I believe other people are too much concerned with online privacy issues. I am concerned about threats to my personal privacy today. All things considered, the Internet would cause serious privacy problems
CFIP	**Errors**	All the personal information in computer databases should be double-checked for accuracy—no matter how much it costs. Companies should have better procedures to correct errors in personal information Companies should devote more time and effort to verifying the accuracy of the personal information in their databases. Companies should take more steps to make sure that the personal information in their files is accurate.
	Unauthorized Use	Companies should not use personal information for any purpose unless it has been authorized by the individuals who provided the information. When people give personal information to a company for some reason, the company should never use the information for any other reason. Companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information. Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.
	Improper Access	Companies should devote more time and effort to preventing unauthorized access to personal information. Computer databases that contain personal information should be protected from unauthorized access—no matter how much it costs. Companies should take more steps to make sure that unauthorized people cannot access personal information in their computers.
IUIPC	**Awareness**	Companies seeking information online should disclose the way the data are collected, processed, and used. A good consumer online privacy policy should have a clear and conspicuous disclosure. Companies should never sell the personal information in their computer databases to other companies. It is very important to me that I am aware and knowledgeable about how my personal information will be used.
	Control	I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction. Consumer control of personal information lies at the heart of consumer privacy. Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.
IUIPC + CFIP	**Collection**	It usually bothers me when (online) companies ask me for personal information. When (online) companies ask me for information, I sometimes think twice before providing it. It bothers me to give personal information to so many (online) companies. I'm concerned that (online) companies are collecting too much personal information about me.

Table 1. The Table shows the privacy scales and their respective statements selected for investigation in this study. (Source: Authors' own work)

Construct	Definition
Privacy `Concern`	An expression of worry towards a specific privacy-related situation.
Privacy `Attitude`	An individual's predisposition towards privacy which influences their stance regarding different privacy-related situations.
Privacy `Preference`	An individual's preferred outcome for a specific privacy-related situation.
Privacy `Expectation`	An expression of what one views as the likely specific privacy-related outcome of a situation or behavior from the other parties involved.
Privacy `Decision`	What an individual chooses to do in a specific privacy-related situation among available options.
Privacy `Behavior`	What an individual actually does or has done in an attempt to achieve the level of privacy that they prefer.

Table 2. Similar to the original study, this table shows the investigated constructs and their respective definitions used in this study. (Source: Colnago et al. [7])

Construct	CFIP	GIPC	IUIPC	Westin	Generated
`attitude`	1/0	2/2	1/1	1/0	4/8
`preference`	0/6	1/1	0/3	0/0	3/6
`concern`	14/6	3/2	6/1	1/1	23/6
`expectation`	0/2	0/0	0/1	1/2	3/6
`decision + behavior`	0/1	0/1	0/0	0/0	6/13

Table 3. The Table shows the breakdown of the number of statements for each meta-construct per source. For reporting, we use the format X/Y, where X shows our results, and Y shows the results from the original study. (Source: Authors' own work)

the interpretation of the statements by the UK sample (RQ1) before detailing the comparison to the US (RQ2). We furthermore detail our data analysis approach. For research transparency and reproducibility, we have made the raw data and the analysis code publicly available at Zenodo [13].

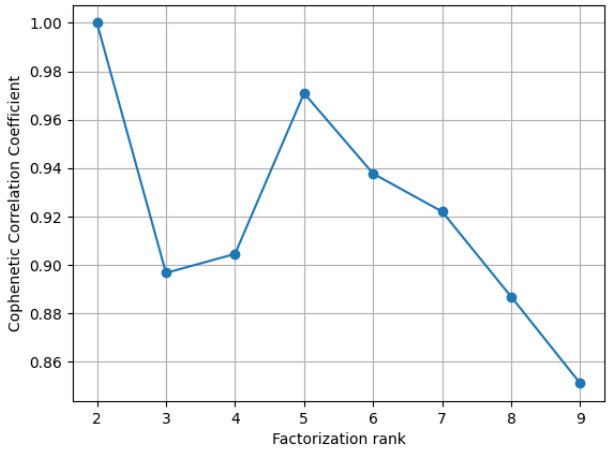

Fig. 1. The Figure shows the Cophenetic correlation coefficient graph (ranks 2–10) indicating a continuous drop for ranks > 5. (Source: Authors' own work)

4.1 Primary Constructs

We replicated the analysis approach of Colnago et al. [7] to identify if each statement had a single primary construct. To ensure direct comparability, this replication entailed first binning participant responses into 'high' (4,5) and 'low' (1,2,3) scores, then identifying the two constructs with the most 'high' responses for each statement. We then compared the distributions of 'high' and 'low' scores between these top two constructs using Chi-square tests. If the top construct had a significantly different distribution ($p < 0.05$) from the second construct, it could be considered the primary construct for that statement. In these cases, we applied Cramer's V to report the effect size in three brackets: low (0.1 - 0.3), medium (0.3 - 0.5) and high (>0.5), where df = 1, reflecting the comparison between the top construct and second-to-top construct. Cramer's V measures the strength of association between two variables, ranging between 0 and 1, where 0 implies no association and 1 implies a perfect relationship. The effect size is used for tests of independence and also for goodness-of-fit tests [6]. Similar to the original study [7], the results of this analysis indicated that a single primary construct did not describe the majority of statements and that those that were often had small effect sizes.

Only 14 of the 70 total statements (20%) had what could be considered a primary construct, with a significantly larger distribution of 'high' than 'low' responses than the next second-highest construct. Of these 14 instances, 4 had a small effect size, and 10 had a medium effect size. Detailed results are presented in the Appendix Table A.3.

4.2 Meta-Constructs

To better understand how the constructs relate to one another and to the statements, we replicated the analysis approach of Colnago et al. [7] using the Non-Negative Matrix Factorization (NMF) algorithm. The NMF algorithm [39, 25] decomposes a matrix into non-negative components, facilitating clustering by uncovering hidden patterns and relationships within the data. In the study context, it allows us to better understand the interrelationships among the constructs and their connections to the statements. Therefore, similar to the original study, we employed this method to identify the construct of each statement captured from the perspective of the user.

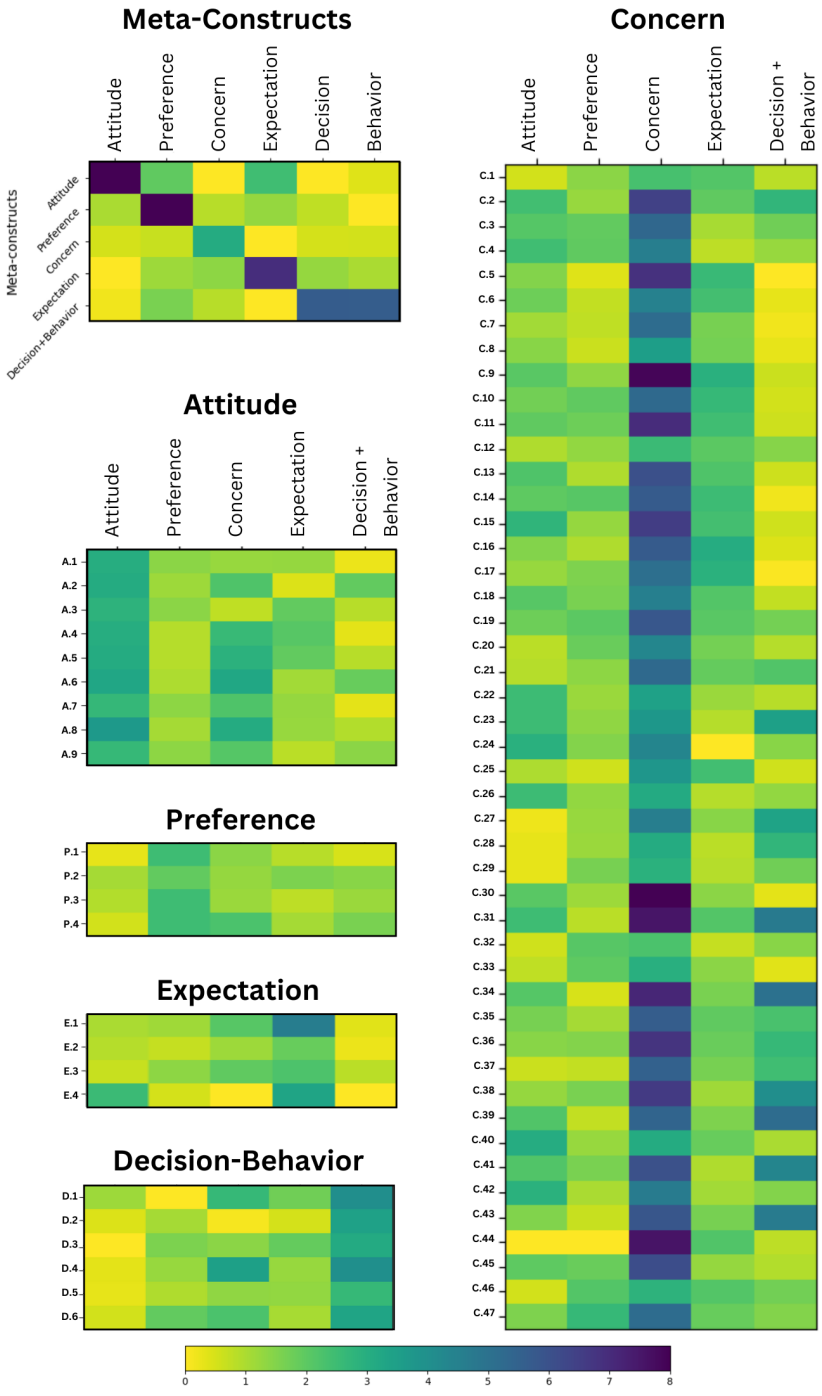

Fig. 2. Heatmap displaying the NMF coefficient results showing the composition of each statement based on the meta-constructs for statements under five constructs: `attitude`, `concern`, `preferences`, `behaviour`, and `decision`. For the list of statements associated with each code, please refer to Appendix A.1. (Source: Authors' own work)

We ran the NMF algorithm on a matrix with six constructs and 70 statements, where each cell indicated the count of participants who selected a 'high' level of agreement ("strongly agree" (5) or "agree" (4)) for each construct-statement pair.

The first step in NMF is selecting the number of components (rank) that produces reliable and meaningful results. To identify the optimal rank, we used the cophenetic correlation coefficient, calculated from the consensus matrix. This matrix represents the average connectivity between data points across multiple NMF runs with random initializations, where each entry reflects how often a pair of data points is grouped together. By aggregating these results, the consensus matrix captures the stability of the clustering assignments, and the cophenetic coefficient quantifies how consistently the data structure is preserved across runs.

We selected the number of ranks needed for stable and descriptive results by examining the cophenetic correlation coefficient graph (Figure 1) [4]. Similar to the original study, we found that when the rank value is 5, the magnitude of the cophenetic correlation coefficient begins to fall. Therefore, we ran the NMF algorithm to output five components, i.e., five meta-constructs. The NMF algorithm associates each statement with a meta-construct. These meta-constructs are composed of the initial constructs, and as shown in Figure 2, they roughly align with the original constructs. Like the original study, privacy behaviour and privacy decisions are grouped into a single meta-construct.

Similar to the original study, our primary constructs seem to lack independence between them and their definitions. As a result, we employed NMF to identify composite constructs. The NMF results display the weighted function of the identified meta-constructs describing each statement (see Figure 2).

4.3 Results Grouped by Scale

In this section, we present our results with statements grouped according to the scale to which they are related. Table 3 summarises the breakdown of meta-constructs by source. The strength of the associations is illustrated in the heatmaps in Figure 2.

CFIP [35]. This scale was designed to measure the construct 'privacy concern'. Perhaps interestingly, we observed that all statements in this scale, except for one, were associated with `concern` as their meta-construct. The only statement not associated with the `concern` meta-construct was, "*I'm concerned that (online) companies are collecting too much personal information about me.*" Instead, this statement was linked to `attitude`. However, the NMF coefficient results for `concern` were high and close to that of `attitude`, indicating that attitude is not dominant, and this statement can still be considered to measure `concern`. In comparison, in the original paper, only 6 out of 15 had privacy `concern` as their meta-construct. Six of the statements had privacy `preferences` as their meta-construct, and none of the meta-constructs was dominant. Overall, the results show that the interpretation of the statements of CFIP matched the linguistic and cultural setting of UK citizens, as opposed to the US. Considering the results, CFIP proves to be a valid construct that accurately measures the intended construct in the UK.

GIPC [27]. We considered privacy concern as the construct intended to be measured by GIPC's statements, as in the original study. Our findings reveal that three of the six GIPC statements indeed relate to `concern`. The statements "*I am concerned about threats to my personal privacy today*" and "*All things considered, the Internet would cause serious privacy problems*" were categorized as `attitude`. Furthermore, the statement "*I am concerned about threats to my personal privacy today*" was classified as `preference`.

Our results greatly differed from the results in the original paper. For example, in the original study, two out of six statements had privacy `concern` as their meta construct, and two had privacy `attitude` as their meta construct.

Furthermore, the US participants perceived the statement "*I am concerned about threats to my personal privacy today*" as measuring concern. In contrast, UK participants perceived it as measuring privacy attitude and preference. To sum up, the statements were perceived differently by the US and the UK citizens; therefore, we cannot establish with certainty if GIPC succeeds in measuring the intended construct.

IUIPC [27]. We considered that the IUIPC was created to capture the privacy concern construct similar to the original study. All statements in this scale were associated with the meta-construct concern, except for two statements: "*I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction*" and "*I'm concerned that (online) companies are collecting too much personal information about me*". These two statements were linked to the attitude meta-construct. In the original study, privacy concern was seen as the meta-construct for only one statement, "*I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.*" Furthermore, three statements were classified as measuring preference in the original study, whereas, in our study, no statement was classified as measuring privacy preference. The results for the IUIPC study in the UK seem to be systematic and follow the expected construct. Similar to the results observed for CFIP, the statements of IUIPC were mostly accurately perceived by the UK audience as intended. However, the opposite was observed in the US. This shows that IUIPC has more external and ecological validity in the UK than in the US. This also indicates that IUIPC and CFIP have precise statement wording in contrast to other scales' statements.

Westin [20]. We considered that Westin's Privacy Segmentation Index was designed to measure privacy concerns. However, our analysis reveals that only one statement in this index was categorized as concern, namely "*Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today*". The statement, "*Consumers have lost all control over how personal information is collected and used by companies*", was associated with attitude meta-construct, and "*Most businesses handle the personal information they collect about consumers properly and confidentially*", was linked with preference. Comparing the results to the original study shows a mismatch between the meta-constructs. For example, the statement "*Consumers have lost all control over how personal information is collected and used by companies*" had privacy concern as the meta-construct in the original study. In contrast, this statement had an attitude as the meta-construct in our study. Another example is the statement, "*Most businesses handle the personal information they collect about consumers properly and confidentially*" which was identified as measuring privacy expectation in the original study and was identified as measuring privacy preference in our study. The differences observed for Westin appeared a bit random, and we cannot establish a systematic difference in the interpretation of the statements and the link between them and each of the constructs.

Expert-Generated statements: 30 statements out of 39 (about 77% of statements) were associated with meta-constructs other than expected. Out of these, 19 statements were expected as attitude, but classified with concern (23.3%, N=7), preference (6.6%, N=2), or decision+behavior (3.3%, N=1). Next, five statements expected as preference were classified as concern (13.3%, N=4) and decision+behavior (3.3%, N=1). Another five statements expected as concern were classified as attitude (10%, N=3) or preference (6.6%, N=2). Further, four statements expected as expectation were classified as concern (10%, N=3), or attitude (3.3%, N=1). Three statements were expected as behavior, but classified as concern (10%) and another three statements expected as decision were also classified as concern (10%). The reader is referred to Appendix A.2 for a full list of the statements.

In the original study by Colnago et al., only six statements (15.4%) were not classified as expected. These statements were also classified differently from those expected in our study. Two of our classifications match the one from Colnago et al., the other four consider the following statements:

- *I don't care about privacy as long as I can use the service.* (Classification: `concern`, Colnago et al.: `behavior+decision`, Expected: `preference`)
- *I don't think there's anything to worry related to privacy.* (Classification: `preferences`, Colnago et al.: `attitude`, Expected: `concern`)
- *I will be able to achieve the level of privacy that I want to have.* (Classification: `concern`, Colnago et al.: `preference`, Expected: `expectation`)
- *Privacy has no place in the modern world.* (Classification: `concern`, Colnago et al.: `expectation`, Expected: `attitude`)

The generated statements were formulated by the US-based researchers who carried out the initial study in the US. While we do not want to speculate about the exact origins of the different results obtained in both studies, we assume that the origin of the researchers who formulated the statements might have contributed to the differences. Table 3 shows the cumulative breakdown of the number of statements for each meta-construct per source in our study and the original study.

> **Results Summary:** Similar to the original study, the results show a significant misalignment in the interpretation of the statements by the UK sample. This indicates that, regardless of the commonality of the primary language of both countries, scale statements are perceived as measuring different constructs by both populations. However, a common observation is that privacy `concern` was the most allocated construct in the US and the UK sample (regardless of the primary classification of the statements). On the contrary, the privacy `behaviour` and `decision` classifications were more prominent in the US than in the UK. Privacy `expectation` and `preference` were more highlighted in the US than in the UK sample. Furthermore, privacy `attitude` appeared almost equally in the US and the UK sample. These observations provide a glimpse of the perception of privacy by the US and UK participants. We discuss the implications of these results in Section 5.

5 DISCUSSION

In this study, we observed that the scale statements differ in measuring the intended construct. The misalignment exists in the US and the UK-based population. The results of the original study by Colnago et al. and the replication study presented in this paper invite the researchers to investigate the cause of the misalignment further and to validate the scales over time with different populations to ensure accurate measurements.

5.1 Misalignment in the Understanding of Scale Statements goes beyond Borders

A common finding between the two studies suggests that no statement uniquely measures the construct it aims to measure. However, there were differences between the US and the UK samples. For example, among the set of generated statements, the expected construct matched almost 85% of the intended constructs in the US-based sample. However, in the UK-based sample, only about 23% of statements matched their expected construct. The IUIPC, CFIP, GIPC, and Westin's Privacy Segmentation Index also observed differences in statement interpretation. While the named scales are well validated and reliable, they are perceived as measuring different constructs. Similarly, differences were also

#	Item Statement	Expected Construct	Our Result
1	Companies create an advertisement profile for each of us that will be used to decide which ads to show us.	Expectation	Expectation
2	Companies that collect and sell data for ad profiles respect users' privacy.	Expectation	Expectation
3	Companies will protect their consumers' data	Expectation	Concern
4	I already take steps to protect my privacy	Behavior	Behavior
5	I am concerned with how much companies are learning about me in order to show me online targeted advertisements.	Concern	Concern
6	I am not satisfied with my current level of privacy	Attitude	Concern
7	I am under surveillance every time I leave the house or go online.	Expectation	Attitude
8	I don't care about privacy as long as I can use the service	Preference	Concern
9	I don't do anything to protect my privacy.	Behavior	Behavior
10	I don't mind that others know what I'm doing	Attitude	Concern
11	I don't think that privacy is important to me	Attitude	Concern
12	I don't think there's anything to worry related to privacy.	Concern	Preference
13	I don't want companies to collect information about me to show me targeted online advertisements.	Preference	Concern
14	I feel that society worries too much about privacy	Attitude	Preference
15	I installed something on my browser to make it harder to track me online	Behavior	Concern
16	I think that others worry too much about privacy	Attitude	Concern
17	I think that privacy is important for society	Attitude	Concern
18	I use private browsing for privacy reasons	Behavior	Concern
19	I want to be able to control what others learn about me	Preference	Concern
20	I want to have a high level of privacy protection.	Preference	Concern
21	I will be able to achieve the level of privacy that I want to have.	Expectation	Concern
22	I will be proactive about protecting my privacy	Decision	Concern
23	I will install software to make it harder for my behavior to be tracked online.	Decision	Concern
24	I will take the privacy level that I am given.	Decision	Decision
25	I won't change any aspect of my online life to protect my privacy.	Decision	Decision+Behavior
26	I worry about not being able to have privacy anymore.	Concern	Concern
27	I worry that online targeted advertisements will disclose details about my preferences and behaviors to others using my computer.	Concern	Attitude
28	I would change how I use the internet to protect my privacy.	Decision	Concern
29	I'm concerned that we, as a society, will lose our privacy.	Concern	Attitude
30	I'm uneasy about the current amount of privacy I have.	Concern	Concern
31	I've opted-out of online targeted advertisement through the NAI (Network Advertising Initiative) website.	Behavior	Concern
32	If I have to see online advertisements, I rather they are targeted to my taste.	Preference	Concern
33	My life is an open book.	Attitude	Decision+Behavior
34	Online companies will collect my data and sell it to advertising companies.	Expectation	Expectation
35	Online targeted advertisements should not be allowed.	Preference	Concern
36	Only people who have something to hide need privacy.	Attitude	Preference
37	Privacy has no place in the modern world.	Attitude	Concern
38	Privacy is a fundamental human right.	Attitude	Concern
39	Privacy is not enough of a reason for me to change how I use the Internet.	Decision	Decision

Table 4. The Table shows the expected and achieved construct of the generated items. The item statements that matched the expected construct are highlighted in green. (Source: Authors' own work)

observed for the investigated scales (IUIPC, CFIP, GIPC, and Westin's Privacy Segmentation). We suspect this could be due to the differences in cultural norms, practices, and data handling [16]. One possible reason could be the introduction of GDPR in the European Union, which was kept by the UK after Brexit and still impacts how people perceive privacy nowadays. This highlights the need for further investigations into the cause of the differences and, more importantly, further investigations into the scale's validity.

Our results suggest that the differences in statement classification and intended construct could be due to a conceptual overlap between construct definitions or due to the evolution of language over time. For example, the IUIPC scale was proposed in 2004, and twenty years after its introduction, there have been several changes in language. Changes in the language could also be impacted by the generational effect; for example, Generation Z and millennials have different linguistic styles [21]. Another underlying reason for the differences could be how the concept of privacy has evolved over time. For example, when smartphones were introduced, people were concerned about the data they would hold [34]; however, now, people are much more confident in their use of smartphones. Moreover, the differences in results also show that the deeper and narrower we go in the construct definition, the harder it is to develop a precise construct definition and its respective statements that ensure accurate measurement.

Another concern that arises from the results is how the understanding of statements changes when the scales developed in an English-speaking country are used for investigation in a non-English-speaking country. While there are differences in understanding between the two English-speaking countries, it can be expected that even more unexpected

results could be observed in non-English-speaking countries. Therefore, there is a need to investigate how the issue of understanding scale statements could be resolved.

5.2 Recommendations for Scale Development & Validation

We make several recommendations for scale development and validation studies based on the results and related work.

- **Pilot Testing of Statements:** First of all, we emphasise and reiterate that scale development includes pilot testing as described in the literature [18, 2, 31]. In the initial phases of scale development, researchers should evaluate the statement's understanding with a sample of the target population. Adding this step as part of the methodology helps minimise the subjective interpretation.
- **Development of Statements:** The statements should be developed with precise wording; for example, avoid lengthy statements and use everyday, commonly used phrases, as they help minimise subjective interpretation [2, 28]. Furthermore, precise wording would also help save the respondent's time, which would ultimately help improve the quality of data collection. The wording of the statements should also be accessible to different literacy levels, as it may impact how well they are understood.
- **Country-Specific Validations:** While developing the scale, researchers should consider starting with one particular country for initial development and validation. After the validation success with one sample, researchers should explore other countries for further validation. This would help control the variations in understanding of the statements. For example, recent work on scale validation shows that scales developed using samples from Western countries might not work when deployed in non-Western countries such as the Middle East and North Africa [14].
- **Assessments over Time:** The differences observed between the US and UK samples could be due to the different timings of the study. Furthermore, with linguistic changes, changes in the interpretation could also be expected. On the other side, the results of this study and the original study present evidence that scales need assessment over time, as emphasised in the original paper by Colnago et al. This guides us that the scales should be validated over time to ensure accurate measurement. Assessment over time ensures that the scale precisely and accurately measures the construct it aims to measure.
- **Indicators of Validity:** Understanding of statements has been identified as one of the crucial steps in ensuring scale validity, as seen in previous work by Colnago et al. [7, 28] and this paper. However, recent research has shown that user interface elements such as response widgets can also impact the scale validity [12]. This indicates that there is a need to be consistent with the user interface style when developing the scales and to have a set of directions for scale deployment as part of the contribution of the scale.

5.3 Limitations

To ensure accurate replication, we carefully replicated all steps of the analysis of the original study. This section reflects the limitations of our paper:

Like all online surveys, our results might suffer from response biases, such as wrong self-assessments. Furthermore, since online questionnaires do not involve interaction with an examiner, participants might have misinterpreted the sentiment behind a question. However, our study and the original study by Colnago et al. aimed to investigate precisely that.

We furthermore want to acknowledge the methodological limitation of utilising NMF and binned-testing for the data analysis. The NMF algorithm can yield different results in different executions due to its random initialisation of the factor matrices, which is influenced by the seed value. The seed value significantly impacts whether the algorithm converges to a global or local minimum, affecting both the speed and quality of convergence. Some seed values lead to faster and better (i.e. lower error) solutions, while others result in slower convergence or suboptimal solutions. We ran the algorithm with various seed values (100 different random values) multiple times to ensure robust findings and analysed the consensus results. We present results that illustrate the common patterns observed across numerous executions. We chose a direct replication of Colnago et al.'s [7] NMF-based methodology to ensure methodological consistency and enable meaningful comparison of findings. For future research exploring construct–statement relationships, alternative methods, such as Latent Dirichlet Allocation (LDA) [1], may offer more robust results.

For binned testing, it may seem counterintuitive to first collect more detailed data on a scale from 1 to 5 and then dichotomise it, as this procedure may lead to loss of variation and, consequently, loss of power for the tests. However, we adopted this approach of data analysis as we wanted to make a direct replication of the work by Colnago et al. However, we recommend that future researchers who do not aim at direct replication consider using the analysis without binning.

Furthermore, while we collected participants' demographic information, including their familiarity with tech, education and profession, we do not draw comparisons of results based on their level of tech familiarity. However, this will be an interesting direction for future work to explore if the level of tech familiarity affects how participants understand and respond to scale questionnaires.

5.4 Guidance for Future Work

This section motivates future work based on the original study, our results, and related work.

Investigation of a non-English speaking audience: Comparing our results with those reported in the study by Colnago et al., we find that even within a language group, the interpretation of statements can broadly differ. Furthermore, translation from one language to another also impacts the understanding of a statement [14]. While official translations of several scales (e.g., UEQ [24]) are available in the non-privacy scope, future work should investigate the perception of the investigated scales in other languages.

Role of Researcher's Background in Item Development: During the item statement formulation stage and statement classification, it might be possible that the researcher's background makes an impact on how the statement is formulated or classified with any construct. To avoid this problem, future scale development studies should incorporate researchers from various backgrounds and then reach a mutual scientific conclusion.

Inclusion of non-WEIRD communities: So far, we have results from investigations in the US and UK, which are Western, educated, industrialised, rich and democratic (short: WEIRD) countries. Besides the integration of languages different from English, we encourage future work in non-WEIRD countries [30, 14].

Developing a privacy glossary: Next, the results of our study and the original study by Colnago et al. emphasise that researchers should design a glossary of statement wordings representing different privacy constructs. This way, scale developers can use the glossary to create new privacy scales and avoid problems with statement interpretations. Furthermore, scales could be built dynamically, and their wording could be tailored to the background of the specific

study participants. Such an approach also requires further steps to establish a solid methodology on dynamic scale development that produces valid results.

6 CONCLUSION

Privacy scales are scientific instruments designed to capture a specific construct. The precise understanding of scale statements is crucial to ensure accurate measurement. In this paper, we replicated a study on the target audience's understanding of privacy scale statements with a UK representative sample. Despite the sample differences between the US and the UK, our results are similar to those of the original study. Both studies show a mismatch between expected and actual statement classification. This may be due to the time-lapse and improvements in language. This highlights the need for scale refinement studies over time. We conclude by discussing recommendations for scale development and validation.

ACKNOWLEDGMENTS

This work was co-funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972, the joint project: digital fitness for citizens - realistic risk perception, secure routines - "DigiFit" - grant number 16KIS1646K, and the program "Digitalisierungprofessuren für Niedersachsen" by the Niedersächsisches Ministerium für Wissenschaft und Kultur. Professor Khamis's time was part-funded by UK Research and Innovation (UKRI) under the UK government's Horizon Europe Funding Guarantee [EP/Z000068/1] (AUGSOC -https://augsoc-project.org/).

REFERENCES

[1] David M Blei, Andrew Y Ng, and Michael I Jordan. "Latent dirichlet allocation". In: Journal of machine Learning research 3.Jan (2003), pp. 993–1022.

[2] Godfred O Boateng et al. "Best practices for developing and validating scales for health, social, and behavioral research: a primer". In: Frontiers in public health 6 (2018), p. 149.

[3] Elijah Robert Bouma-Sims et al. "A US-UK Usability Evaluation of Consent Management Platform Cookie Consent Interface Design on Desktop and Mobile". In: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems. CHI '23. Hamburg, Germany: Association for Computing Machinery, 2023. ISBN: 9781450394215. DOI: 10.1145/3544548.3580725. URL: https://doi.org/10.1145/3544548.3580725.

[4] Jean-Philippe Brunet et al. "Metagenes and molecular pattern discovery using matrix factorization". In: Proceedings of the national academy of sciences 101.12 (2004), pp. 4164–4169.

[5] Paul Cairns. Doing better statistics in human-computer interaction. Cambridge University Press, 2019. ISBN: 978-1108482523.

[6] Jacob Cohen. Statistical power analysis for the behavioral sciences. routledge, 2013.

[7] Jessica Colnago et al. "Is it a concern or a preference? An investigation into the ability of privacy scales to capture and distinguish granular privacy constructs". In: Eighteenth Symposium on Usable Privacy and Security. SOUPS 2022. Berkeley, US: Usenix Association, 2022, pp. 331–346.

[8] Lee J. Cronbach and Paul E. Meehl. "Construct validity in psychological tests." In: Psychological bulletin 52.4 (1955), p. 281.

[9] Cori Faklaris, Laura A Dabbish, and Jason I Hong. "A self-report measure of end-user security attitudes (SA-6)". In: Proceedings of the Fifteenth Symposium on Usable Privacy and Security. SOUPS 2019. Berkeley, US: Usenix Association, 2019, pp. 61–77.

[10] Habiba Farzand, Karola Marky, and Mohamed Khamis. "Out-of-Device Privacy Unveiled: Designing and Validating the Out-of-Device Privacy Scale (ODPS)". In: Proceedings of the CHI Conference on Human Factors in Computing Systems. CHI

'24. Honolulu, HI, USA: Association for Computing Machinery, 2024. ISBN: 9798400703300. DOI: 10.1145/3613904.3642623. URL: https://doi.org/10.1145/3613904.3642623.

[11] Habiba Farzand et al. "A Systematic Deconstruction of Human-Centric Privacy & Security Threats on Mobile Phones". In: International Journal of Human–Computer Interaction (2024), pp. 1–24.

[12] Habiba Farzand et al. "Beyond Aesthetics: Evaluating Response Widgets for Reliability & Construct Validity of Scale Questionnaires". In: Extended Abstracts of the 2024 CHI Conference on Human Factors in Computing Systems. CHI EA '24. Association for Computing Machinery, 2024. ISBN: 9798400703317. DOI: 10.1145/3613905.3650751. URL: https://doi.org/10.1145/3613905.3650751.

[13] Habiba Farzand et al.
Revisiting Privacy Scales: An investigation into An Investigation into the Ability of Privacy Scales to Capture & Distinguish Granular Privacy Cons
Version 1.0. Zenodo, June 2025. DOI: 10.5281/zenodo.15741904. URL: https://doi.org/10.5281/zenodo.15741904.

[14] Habiba Farzand et al. "When Scales Fail to Measure up: How Not to Measure Social Media Privacy: Findings of a Representative Survey in 16 Countries". In:
Extended Abstracts of the CHI Conference on Human Factors in Computing Systems. 2025, pp. 1–9.

[15] Thomas Groß. "Validity and reliability of the scale internet users' information privacy concerns (iuipc)". In: Proceedings on Privacy Enhancing Technologies (2021).

[16] Calin Gurau, Ashok Ranchhod, and Claire Gauzente. ""To legislate or not to legislate": a comparative exploratory study of privacy/personalisation factors affecting French, UK and US Web sites". In: Journal of consumer Marketing 20.7 (2003), pp. 652–664.

[17] Eszter Hargittai and Eden Litt. "New strategies for employment? internet skills and online privacy practices during people's job search". In: IEEE security & privacy 11.3 (2013), pp. 38–45.

[18] Rakibul Hasan et al. "A Psychometric Scale to Measure Individuals' Value of Other People's Privacy (VOPP)". In: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems. 2023, pp. 1–14.

[19] Franziska Herbert et al. "A world full of privacy and security (mis) conceptions? Findings of a representative survey in 12 countries". In: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems. 2023, pp. 1–23.

[20] Harris Interactive. "Privacy on and off the Internet: What consumers want". In: Privacy and American Business (2002), pp. 1–127.

[21] Ana Juli, Marina Suci, and Apriyani Esti. "Comparison Of Slang In Millennials And Gen Z: A Semantic Analysis In The Context Of Linguistic Learning". In: Semantik: Jurnal Riset Ilmu Pendidikan, Bahasa dan Budaya 2.3 (2024), pp. 206–215.

[22] Yoojung Kim, Dongyoung Sohn, and Sejung Marina Choi. "Cultural difference in motivations for using social network sites: A comparative study of American and Korean college students". In: Computers in human behavior 27.1 (2011), pp. 365–372.

[23] 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. IEEE. 2010, pp. 1–10.

[24] Bettina Laugwitz, Theo Held, and Martin Schrepp. "Construction and Evaluation of a User Experience Questionnaire". In: Proceedings of the Symposium of the Austrian HCI and Usability Engineering Group (USAB). Cham, Switzerland: Springer, 2008, pp. 63–76. DOI: 10.1007/978-3-540-89350-9_6.

[25] Tao Li and Chris Ding. "The relationships among various nonnegative matrix factorization methods for clustering". In: Proceedings of the Sixth International Conference on Data Mining. ICDM'06. IEEE. 2006, pp. 362–371.

[26] Yao Li et al. "Cross-cultural privacy prediction". In: Proceedings on Privacy Enhancing Technologies (2017).

[27] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model". In: Information Systems Research 15.4 (2004), pp. 336–355.

[28] Fabiane FR Morgado et al. "Scale development: ten main limitations and recommendations to improve future research practices". In: Psicologia: Reflexão e Crítica 30.0 (2017), p. 3.

[29] Office of National Statistics. UK Office of National Statistics. Retrieved July 11, 2024. 2024. URL: https://www.ons.gov.uk.

[30] Sheza Naveed et al. "" Ask this from the person who has private stuff": Privacy Perceptions, Behaviours and Beliefs Beyond WEIRD". In: Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems. 2022, pp. 1–17.

[31] Heather L O'Brien and Elaine G Toms. "The development and evaluation of a survey to measure user engagement". In: Journal of the American Society for Information Science and Technology 61.1 (2010), pp. 50–69.

[32] Prolific. Prolific | Online participant recruitment for surveys and market research. Retrieved May 28, 2024. 2024. URL: https://www.prolific.co/.

[33] Mennatallah Saleh, Mohamed Khamis, and Christian Sturm. "What About My Privacy, Habibi?" In: IFIP Conference on Human-Computer Interaction. Springer. 2019, pp. 67–87.

[34] Katie Shilton. "Four billion little brothers? Privacy, mobile phones, and ubiquitous data collection". In: Communications of the ACM 52.11 (2009), pp. 48–53.

[35] H. Jeff Smith, Sandra J. Milberg, and Sandra J. Burke. "Information privacy: Measuring individuals' concerns about organizational practices". In: MIS quarterly (1996), pp. 167–196.

[36] Sabine Trepte et al. "A cross-cultural perspective on the privacy calculus". In: Social Media+ Society 3.1 (2017), p. 2056305116688035.

[37] Alan F. Westin. "Privacy and freedom". In: Washington and Lee Law Review 25.1 (1968), p. 166.

[38] Allison Woodruff et al. "Would a Privacy Fundamentalist Sell Their DNA for 1000...If Nothing Bad Happened as a Result? The Westin Categories, Behavioral Intentions, and Consequences". In: Proceedings of the 10th Symposium On Usable Privacy and Security. SOUPS 2014. Berkeley, Us: Usenix Association, 2014, pp. 1–18.

[39] Wei Xu, Xin Liu, and Yihong Gong. "Document clustering based on non-negative matrix factorization". In: Proceedings of the 26th annual international ACM SIGIR conference on Research and development in informaion retrieval. 2003, pp. 267–273.

A APPENDIX

A.1 Statements of the Heatmaps

- **A.1:** Consumers have lost all control over how personal information is collected and used by companies
- **A.2:** I am concerned about the threats to my personal privacy today
- **A.3:** All things considered, the Internet would cause serious privacy problems
- **A.4:** I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of marketing transaction
- **A.5:** I am concerned that (online) companies are collecting too much personal information about me
- **A.6:** I am concerned with how much companies are learning about me in order to show me online targeted advertisements
- **A.7:** I am under surveillance every time I leave the house or go online
- **A.8:** I worry that online targeted advertisements will disclose details about my preferences and behaviors to others using my computer
- **A.9:** I am concerned that we, as a society, will lose our privacy
- **P.1:** I believe other people are too much concerned with online privacy issues
- **P.2:** I don't think there's anything to worry about privacy
- **P.3:** I feel that society worries too much about privacy
- **P.4:** Only people who have something to hide need privacy

- **E.1:** Most businesses handle the personal information they collect about consumers in a proper and confidential way
- **E.2:** Companies create an advertisement profile for each of us that will be used to decide which ads to show us
- **E.3:** Companies that collect and sell data for ad profiles respect users' privacy
- **E.4:** Online companies will collect my data and sell it to advertising companies
- **D.1:** I already take steps to protect my privacy
- **D.2:** I don't do anything to protect my privacy
- **D.3:** I will take the privacy level I am given
- **D.4:** I won't change any aspect of my online life to protect my privacy
- **D.5:** My life is an open book
- **D.6:** Privacy is not enough of a reason for me to change how I use the internet
- **C.1:** Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today
- **C.2:** To me it is the most important thing to keep my privacy intact from online companies
- **C.3:** Compared with other subjects in mind, personal privacy is very important
- **C.4:** Compared to others, I am more sensitive about the way online companies handle my personal information
- **C.5:** All the personal information in computer databases should be double-checked for accuracy–no matter how much it costs
- **C.6:** Companies should have better procedures to correct errors in personal information
- **C.7:** Companies should devote more time and effort to verifying the accuracy of personal information in their databases
- **C.8:** Companies should take more steps to make sure that the personal information in their files is accurate.
- **C.9:** Companies should not use personal information for any purpose unless it has been authorized by the individuals who provided the information.
- **C.10:** When people give personal information to a company for some reason, the company should never use the information for any other reason.
- **C.11:** Companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.
- **C.12:** Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.
- **C.13:** Companies should devote more time and effort to preventing unauthorized access to personal information.
- **C.14:** Computer databases that contain personal information should be protected from unauthorized access—no matter how much it costs.
- **C.15:** Companies should take more steps to make sure that unauthorized people cannot access personal information in their computers.
- **C.16:** Companies seeking information online should disclose the way the data are collected, processed, and used.
- **C.17:** A good consumer online privacy policy should have a clear and conspicuous disclosure.
- **C.18:** Companies should never sell the personal information in their computer databases to other companies.
- **C.19:** It is very important to me that I am aware and knowledgeable about how my personal information will be used.
- **C.20:** Consumer control of personal information lies at the heart of consumer privacy.

- **C.21:** Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared
- **C.22:** It usually bothers me when (online) companies ask me for personal information
- **C.23:** When (online) companies ask me for information, I sometimes think twice before providing it.
- **C.24:** It bothers me to give personal information to so many (online) companies.
- **C.25:** Companies will protect their consumers' data
- **C.26:** I am not satisfied with my current level of privacy
- **C.27:** I don't care about privacy as long as I can use the service
- **C.28:** I don't mind that others know what I'm doing
- **C.29:** I don't think that privacy is important to me
- **C.30:** I don't want companies to collect information about me to show me targeted online advertisements.
- **C.31:** I installed something on my browser to make it harder to track me online
- **C.32:** I think that others worry too much about privacy
- **C.33:** I think that privacy is important for society
- **C.34:** I use private browsing for privacy reasons
- **C.35:** I want to be able to control what others learn about me
- **C.36:** I want to have a high level of privacy protection.
- **C.37:** I will be able to achieve the level of privacy that I want to have.
- **C.38:** I will be proactive about protecting my privacy
- **C.39:** I will install software to make it harder for my behavior to be tracked online.
- **C.40:** I worry about not being able to have privacy anymore.
- **C.41:** I would change how I use the internet to protect my privacy.
- **C.42:** I'm uneasy about the current amount of privacy I have.
- **C.43:** I've opted-out of online targeted advertisement through the NAI (Network Advertising Initiative) website.
- **C.44:** If I have to see online advertisements, I rather they are targeted to my taste.
- **C.45:** Online targeted advertisements should not be allowed.
- **C.46:** Privacy has no place in the modern world.
- **C.47:** Privacy is a fundamental human right.

A.2 Results: Generated Statements Primary & Expected Classification

The following list presents the statements that differed from their expected construct.

(1) Companies will protect their consumers' data. (Classification: concern, Expected: expectation)
(2) I am concerned with how much companies are learning about me in order to show me online targeted advertisements. (Classification: attitude, Expected: concern)
(3) I am not satisfied with my current level of privacy. (Classification: concern, Expected: attitude)
(4) I am under surveillance every time I leave the house or go online. (Classification: attitude, Expected: expectation)
(5) I don't care about privacy as long as I can use the service.(Classification: *concern*, Expected: preference)
(6) I don't mind that others know what I'm doing. (Classification: concern, Expected: attitude)
(7) I don't think that privacy is important to me (Classification: concern, Expected: attitude)
(8) I don't think there's anything to worry related to privacy. (Classification: *preferences*, Expected: concern)

(9) I don't want companies to collect information about me to show me targeted online advertisements. (Classification: concern, Expected: preference)
(10) I feel that society worries too much about privacy. (Classification: preference, Expected: attitude)
(11) I installed something on my browser to make it harder to track me online. (Classification: concern, Expected: behaviour)
(12) I think that others worry too much about privacy. (Classification: concern, Expected: attitude)
(13) I think that privacy is important for society. (Classification: concern, Expected: attitude)
(14) I use private browsing for privacy reasons. (Classification: concern, Expected: behaviour)
(15) I want to be able to control what others learn about me. (Classification: concern, Expected: preference)
(16) I want to have a high level of privacy protection. (Classification: concern, Expected: Preference)
(17) I will be able to achieve the level of privacy that I want to have. (Classification: *concern*, Expected: expectation)
(18) I will be proactive about protecting my privacy. (Classification: concern, Expected: decision)
(19) I will install software to make it harder for my behaviour to be tracked online. (Classification: concern, Expected: decision)
(20) I won't change any aspect of my online life to protect my privacy. (Classification: decision+behavior, Expected: Decision)
(21) I worry that online targeted advertisements will disclose details about my preferences and behaviours to others using my computer. (Classification: attitude, Expected: concern)
(22) I would change how I use the internet to protect my privacy. (Classification: concern, Expected: decision)
(23) I'm concerned that we, as a society, will lose our privacy. (Classification: attitude, Expected: concern)
(24) I've opted-out of online targeted advertisement through the NAI (Network Advertising Initiative) website. (Classification: concern, Expected: behaviour)
(25) If I have to see online advertisements, I rather they are targeted to my taste. (Classification: concern, Expected: preference)
(26) My life is an open book. (Classification: decision+behavior, Expected: attitude)
(27) Online targeted advertisements should not be allowed. (Classification: concern, Expected: preference)
(28) Only people who have something to hide need privacy. (Classification: preference, Expected: attitude)
(29) Privacy has no place in the modern world. (Classification: *concern*, Expected: attitude)
(30) Privacy is a fundamental human right. (Classification: concern, Expected: attitude)

A.3 Chi-Square test p-values & Cramer's V effect sizes

Statement	ChiSq p-value	Cramer's V	Statement	ChiSq p-value	Cramer's V
A.01	0.0173	0.2964	C.27	0.6552	0.0740
A.02	0.0099	0.3297	C.28	1.0000	0.0263
A.03	0.1533	0.1886	C.29	0.2435	0.1627
A.04	0.0859	0.2222	C.30	0.6363	0.0793
A.05	0.0317	0.2669	C.31	0.7963	0.0577
A.06	0.0048	0.3373	C.32	0.0129	0.3034
A.07	0.0715	0.2462	C.33	0.1119	0.2057
A.08	0.0001	0.4698	C.34	1.0000	0.0334
A.09	0.1294	0.2085	C.35	1.0000	0.0260
C.01	1.0000	0.0000	C.36	1.0000	0.0255
C.02	0.8062	0.0556	C.37	0.8228	0.0501
C.03	0.6511	0.0740	C.38	0.5400	0.1083
C.04	1.0000	0.0281	C.39	1.0000	0.0401
C.05	0.6367	0.0813	C.40	0.1130	0.2901
C.06	0.8111	0.0563	C.41	1.0000	0.0284
C.07	0.4933	0.1034	C.42	0.0306	0.2720
C.08	1.0000	0.0000	C.43	1.0000	0.0000
C.09	0.6097	0.0867	C.44	0.0138	0.3004
C.10	0.8102	0.0544	C.45	0.8209	0.0500
C.11	1.0000	0.0000	C.46	0.1830	0.1716
C.12	1.0000	0.0270	C.47	0.0103	0.3237
C.13	0.8195	0.0510	D.01	0.1341	0.2005
C.14	0.6175	0.0859	D.02	0.6502	0.0770
C.15	0.1928	0.1793	D.03	0.5044	0.0983
C.16	0.6524	0.0746	D.04	0.1130	0.2000
C.17	0.6552	0.0740	D.05	0.6275	0.0883
C.18	1.0000	0.0000	D.06	1.0000	0.0249
C.19	0.3443	0.1322	E.01	0.0002	0.4257
C.20	0.3573	0.1320	E.02	0.3411	0.1347
C.21	1.0000	0.0000	E.03	1.0000	0.0245
C.22	0.1268	0.2129	E.04	0.3346	0.1348
C.23	0.6275	0.0824	P.01	0.0021	0.3895
C.24	0.0537	0.2427	P.02	0.1685	0.1843
C.25	0.4956	0.1029	P.03	0.0029	0.3684
C.26	0.3547	0.1310	P.04	0.0037	0.3500

Table 5. Chi-square test p-values and Cramer's V effect sizes for each statement. Statements with a significant p-value (< 0.05) could be considered to have a primary construct. Effect size brackets where df = 1: low (0.1 - 0.3), medium (0.3 - 0.5) and high (>0.5) (Source: Authors' own work)