A Psychometric Scale to Measure Individuals' *Value of Other People's Privacy* (VOPP)

Rakibul Hasan*
Rakibul.Hasan@asu.edu
Arizona State University, School of Computing and Augmented Intelligence
Tempe, Arizona, USA

Rebecca Weil
Rudolf Siegel
Katharina Krombholz
weil@cispa.de
siegel@cispa.de
krombholz@cispa.de
CISPA Helmholtz Center for Information Security
Saarbrücken, Germany

ABSTRACT

Researchers invested enormous efforts to understand and mitigate the concerns of users as technologies collect their private data. However, users often undermine *other* people's privacy when, e.g., posting other people's photos online, granting mobile applications to access contacts, or using technologies that continuously sense the surrounding. Research to understand technology adoption and behaviors related to collecting and sharing data about non-users has been severely lacking. An essential step to progress in this direction is to identify and quantify factors that affect technology's use. Toward this goal, we propose and validate a psychometric scale to measure how much an individual values *other* people's privacy. We theoretically grounded the appropriateness and relevance of the construct and empirically demonstrated the scale's internal consistency and validity. This scale will advance the field by enabling researchers to predict behaviors, design adaptive privacy-enhancing technologies, and develop interventions to raise awareness and mitigate privacy risks.

CCS CONCEPTS

• **Security and privacy** → *Economics of security and privacy*; **Privacy protections**; **Social aspects of security and privacy**.

KEYWORDS

Privacy, Data tracking, Scale development, Other people, Technology adoption

ACM Reference Format:
Rakibul Hasan, Rebecca Weil, Rudolf Siegel, and Katharina Krombholz. 2023. 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 (CHI '23), April 23–28, 2023, Hamburg, Germany*. ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3544548.3581496

CHI '23, April 23–28, 2023, Hamburg, Germany

ACM ISBN 978-1-4503-9421-5/23/04…$15.00
https://doi.org/10.1145/3544548.3581496

1 INTRODUCTION

Many technologies facilitate, and even encourage, the collection and sharing of data about people other than their users, raising a plethora of privacy issues for the data subjects. For example, online sharing of images and videos taken in public places reveals the identity, location, and other sensitive information about the surrounding people, including uninvolved bystanders [1, 22, 33, 40]. Mobile applications may access details of the saved contacts; such data may be used for spamming and phishing attacks or linked to other data sources for identification and tracking [66]. Smart home cameras surveil domestic workers, guests, and passers by [13, 101] and the recorded data can be shared publicly [51, 62]. Donated genome data can be used to identify others in the family tree [6, 81], potentially risking their privacy and safety, as well as subjecting them to discrimination during applying for jobs, insurances, or loans [5]. The more we move towards a technology-driven and "connected" society, the more privacy issues are becoming "interdependent", where an individual's privacy is contingent on other people's technology use or data-sharing activities [14, 44].

Beyond threatening privacy, safety, and equal treatment at an individual level, interdependent privacy issues can result in social and national challenges as collecting non-users' data (i.e., second-order surveillance) can rapidly scale up the number of people "under watch." Publicly accessible bio-metric and behavioral data can be harvested and abused by anyone with sufficient computing power. A recent example is *ClearView*, a technology company that scraped billions of images and built facial recognition and tracking services [37]. Privacy scholars and activists labeled ClearView's emergence as the "end of privacy" [4], and their product has been announced as a "threat to the black community" by Sen. Edward Markey [16] as facial recognition systems discriminate against people of color and other minority groups.

Research on understanding and mitigating interdependent privacy issues has is limited relative to the significance of the problem. Past research investigated data subjects' concerns for privacy in different contexts—online platforms [68], wearable devices and drones [22, 95], and IoT devices [12, 101]—and proposed privacy enhancing technologies (PETS) to address some of those concerns (e.g., [1, 21]).

In interdependent privacy contexts, however, data subjects can rarely exert any control over sharing their information (e.g., bystanders in photos taken in public places [33]) and often remain

unaware of data collection or sharing (e.g., when mobile apps are provided access to other people's contact details [66]). Past research invented both PETS (e.g., [33–35]) and behavioral interventions [56] to aid technology users in protecting data subjects' privacy, but saw limited success. One study even reported paradoxical findings: priming people to consider data subjects' privacy before sharing photos online *increased* (as opposed to decreased) their willingness to post photos [3]. Unfortunately, our understanding of why technology users behave in certain ways and what personal factors determine such behaviors in interdependent privacy contexts remains severely lacking.

In this paper, we define such a factor and propose a scale to measure it—the essential first step in understanding and predicting behaviors. Concretely, we posit that how much technology users *value* data subjects' privacy plays a key role in exhibiting related behaviors. Accordingly, we define the construct *value of other people's privacy* as the importance that a person ascribes to the protection of others' personal information, and propose and validate a psychometric scale to measure it.

Our construct is grounded in Schwartz's seminal work on universal human values [75]; the *Theory of Basic Human Values* identified 10 fundamental values that guide people's life. Personal values motivate individuals to act in either self-interest or in the interest of other people (altruistic values). Based on the literature, we posit that altruistic behaviors, such as protecting other people's privacy, are strongly influenced by people's other-regarding values [65, 78, 79].

Additionally, the *value* construct transcend, per definition, specific situations [75]; consequently, it is less context-dependent compared to other commonly studied constructs such as *privacy concerns* and *privacy attitudes* [52, 70, 71, 74]. Indeed, recent research demonstrated that the measurement of popular constructs, such as privacy preferences and privacy concerns, suffers from reliability issues [19, 30]. Thus, we argue that *the value of other's privacy* should be more reliable and consistent in predicting behaviors in interdependent privacy contexts than other constructs, and provide an instrument to empirically test this assumption.

In summary, we make the following contributions:

(1) We propose a new construct—*value of other people's privacy*—to measure how much importance people ascribe to the protection of other people's privacy. We provide theoretical reasoning for why this construct is an important factor affecting behaviors in interdependent privacy contexts.
(2) To quantify the construct, we developed and validated a psychometric scale named *VOPP*. Through three studies (total $N = 1450$), we evaluated its internal consistency as well as convergent and discriminant validity.
(3) To establish the scale's ability to predict behaviors, we additionally measured its criteria validity. The scale correlated with self-reported privacy behaviors in an expected manner.

Our scale lays an important foundation to make privacy values measurable for systematic analysis and comparison. This quantification will also allow researchers and technology developers to predict users' behaviors and proactively intervene to protect the private data of non-users.

2 BACKGROUND AND LITERATURE REVIEW

In the following, we outline related research to embed the suggested construct of the value of other people's privacy into existing value theories, distinguish the construct of values from other constructs often referred to in privacy research (i.e., attitudes and concerns), and discuss existing scales proposed to tap into the interdependent nature of privacy issues.

2.1 Challenges for the Development of a Privacy Scale

Several scales exist to measure individuals' concerns, attitudes, and behaviors related to their own privacy [11, 17, 53, 84]. Constructs, commonly found in the privacy literature, assumed to underlie such scales, are *privacy attitudes*, *privacy preferences*, *privacy concerns*, *privacy expectations*, *privacy decisions*, and *privacy behaviors* [19]. However, recent research showed that there seems to be a gap between what privacy scales intend to measure and how they are understood by individuals answering such scales [19]. Consequently, one main challenge in the development of a privacy scale is to ensure that the selected scale items represent the construct that the scale intends to measure. We address this challenge in the present project. A second challenge in the development of a privacy scale relates to a potential dissociation between the implications of the results of a scale and actual privacy behavior [29], because the usefulness of a scale strongly depends on its predictive power. The two challenges are not unrelated and we outline in the following how differences in the assessed construct can influence the predictive power of a scale.

2.2 Value and Related Constructs

We distinguish between concerns about, attitudes towards, and value of others' privacy. Values refer to what is important, good, and worthy [97]. Personal values are desirable and stable goals that influence people's preferences and motivate behaviors across situations [71]. Accordingly, values remain relevant across contexts and over time. In contrast, attitudes reflect people's beliefs, preferences (e.g, likes and dislikes) and behavioral intentions towards an object (e.g., person, topic, event) [92]. Attitudes, differently from values, can be context sensitive [70]. Importantly, attitudes can be value-expressive [52]. That is, a person might adopt and endorse a certain positive or negative attitude as a consequence of an associated value. Hence, values may underlie attitudes [2]. Concerns can be considered a specific type of attitude, namely a negative affect toward a certain attitude object [74]. That is, someone might be concerned (negative affect) about the privacy of others (attitude object) in a certain context, which in turn might motivate a certain behavior in that context, but this concern could be driven by an underlying cross-contextual value of privacy of others. Taken together, assessing other people's privacy as a value enables a more reliable prediction of behaviors related to protecting other people's privacy compared to attitudes, given that values are considered more stable and less context-dependent as compared to attitudes.

2.3 The Theory of Basic Human Values

The idea that values motivate behavior has been previously discussed in the literature [9]. Schwartz's Theory of Basic Human

Values	
socially-focused	**personal-focused**
Self-transendence	*Openness to change*
Universalism	Hedonism
Benevolence	Stimulation
	Self-direction
Conservation	*Self-enhancement*
Security	Achievement
Conformity	Power
Tradition	

Table 1: Categorization of the ten Basic Human Values according to [75].

Values [75] identified 10 fundamental values (i.e., self-direction, stimulation, hedonism, achievement, power, security, conformity, tradition, benevolence, universalism) that guide people's life (and later extended to 19 finer-grained values under the ten coarse-grained values [77]). These values, which have been recognized in at least 30 different countries, fall under two higher-order dimensions: self-transcendence vs. self-enhancement and openness to change vs. conservation. Each dimension represents a basic human conflict, regulating personal interests and relations to other people [76]. The self-transcendence (combining the values *universalism* and *benevolence*) and conservation (combining the values *security*, *conformity*, and *tradition*) poles of the dimensions generally motivate altruistic or prosocial behaviors [65, 80], or in other words, behaviors that are socially-focused and in the interest of other people rather than personal-focused and in the interest of the self [28] (see also Table 1). The assumed role of values for the motivation of behavior which is primarily in the interest of other people is central to the current research context: in interdependent privacy contexts, data subjects can rarely exert any control over the collection or dissemination of their data, and thus have to rely on the technology users' altruism to protect their privacy by, e.g., limiting the use of technology or adopting privacy-enhancing technologies, or both, to lower risk of privacy violations.

2.4 Interdependent Privacy

Interdependent privacy has been investigated in the past. For example in the context of social media [85], especially with respect to online photo sharing [3, 32, 60], and in the context of IoT devices [27]. Typically, when self and other people's privacy needs have to be negotiated [54, 91], users experience conflicts because functional needs, as well as self and other privacy preferences rarely align [88]. To mitigate such conflicts, tools and strategies have been developed aimed at raising awareness for the interdependent nature of privacy issues and resulting consequences [43, 55]. Moreover, these tools and strategies provide users with means to regulate conflicts by offering privacy enhancing measures [72, 83, 87, 102, 104]. Yet, while the motivational background for the adoption of such measures for the protection of one's own privacy is straightforward [99, 100], understanding the motivation to use such measures to protect others remains a key component in understanding interdependent privacy conflicts.

2.5 Related Scales and Topical Findings in the Literature

The importance of acknowledging the interdependent nature of privacy and related issues is highlighted by several studies devoted to understanding and measuring privacy concerns and attitudes. Wirth et al. examined how concerns' for own and other people's privacy and perceived enjoyment from information disclosure influence a co-owner's willingness to protect the original owner's privacy [98]. Pu and Grossklags studied how much interdependent privacy contributes to people's decision in adopting social media relative to other factors [66], and Koohikamali et al. investigated how concerns about other people's privacy, together with social norms and attitudes toward using social networks affect people's intention and behaviors regarding data sharing [48]. Baruh and Cemalcılar developed a privacy orientation scale to measure information sharing and seeking behaviors on social media [11]. Most relevant for the present context, the researchers found that concerns about other people's privacy impact how one observes information shared by other people. The idea that values might play a role in interdependent privacy contexts was suggested in a study in which the authors quantified people's value of one's own and a friend's privacy in terms of money [67]. Thus, while the significance of values for the understanding of interdependent privacy contexts has been addressed previously, our project is the first to propose a psychometric measure to quantify the value of others' privacy directly, rather than only approximating it (e.g., using money as a proxy for personal value).

3 DEVELOPMENT OF THE SCALE

To develop the scale, we implemented a nine-step procedure of scale development that fall under three broad categories of activities: 1) Item development, 2) Scale development, and 3) Scale validation [15]. At each step, we adhered to the best practices described in the scale-development literature [15, 61] and past research that proposed instruments to measure privacy- and security-related constructs (e.g., [11, 24, 25, 48]). The steps are listed below and detailed in the following sections.

Step 1a. *Identification of the construct and item generation:* Define the target construct and create the initial item pool that describes the construct.

Step 1b. *Assess content validity:* Verify whether the items are relevant to and representative of the construct and whether they apply to the actual experiences of the target population.

Step 1c. *Pre-test questions:* Assess the extent to which questions reflect the construct and the response options produce valid measurements.

Step 2a. *Survey administration:* Collect data by surveying a representative sample of the target population.

Step 2b. *Item reduction:* Remove items that do not represent the construct well or are inconsistent with other items.

Step 2c. *Identifying the factor structure:* Identify the latent factors of the scales.

Step 3a. *Confirming the factor structure:* Confirm the identified factor structure with a new sample of data.

Step 3b. *Test of reliability:* Evaluate the scale's internal consistency: the degree to which the set of items agree with each other (i.e., they all measure the same latent factor).

Step 3c. *Tests of validity:* Evaluate the correlation with other scales measuring "similar" constructs and distinctiveness from scales that are supposed to measure "unrelated" constructs.

4 ITEM DEVELOPMENT

4.1 Identification of the Target Construct and Item Generation

In the following, we define the target construct and detail the creation of the initial item pool that describes the construct. A construct or domain refers to the concept, attribute, or unobserved behavior that the study aims to examine [36] and should be defined before creating or collecting the indicating items [69]. Our objective is to develop a scale assessing to which level people exhibit a value of other people's privacy, where "other people" refers to any data subject including family members, friends, colleagues, or strangers around us. That is, we aim to assess how much importance an individual ascribes to the protection of other people's privacy (irrespective of how much value the other people ascribe to their own privacy). We defined "other people" broadly so that the meaning of "others" becomes tantamount to the meaning of "not me (but everyone else)". As such, we do not aim to differentiate between data subjects with various levels of personal or social distance [31, 86]. We defined the construct *value of other people's privacy* before creating items to ensure that the items represent all aspects of the definition. Although we identify and evaluate the number of latent factors that our target domain contains based on empirical data, at this stage, we aim for a single-factor domain as it is considered to be more consistent and reliable than more complex or composite constructs [15, 19, 57]. Toward this goal, we took the utmost care to define the domain boundary to reduce overlaps with other related constructs (e.g., privacy attitudes and self-privacy concerns). After defining the construct, we obtained feedback from security and privacy researchers at our institutes and researchers who specialize in scale development. Their suggestions were instrumental in revising the construct to a basic definition while clarifying all essential features of the domain, and avoiding unreliability issues with composite or vaguely defined constructs [15, 19]. Thus, we defined the construct in the following way:

> The value of other people's privacy is defined as the importance a person ascribes to the protection of other people's personal information. This entails also the ascription of importance to behaviors that are associated with protecting or putting at risk other people's personal information.

As such, the definition does not include the ascription of importance to the protection of one's own privacy and the perception of how important others deem the protection of their own privacy. Moreover, privacy is defined as the protection of personal information.

To make the process of item creation, selection, and refinement transparent and comprehensible, we published all steps and the corresponding items at https://osf.io/q5y4d/.

4.2 Initial Item Pool Generation

To generate the initial item pool, we followed a mixed approach of deductive (i.e., deriving items from a theoretical perspective based on, e.g., a literature review) and inductive (i.e., creation of items by asking people how they perceive a certain topic or behavior [39]) that has been recommended as a better alternative to following either approach independently [15, 39, 59]. Specifically, items were collected in three different ways. First, we derived items by reviewing the existing literature; in particular, we adapted two items that belong to the subscale "Concern about the privacy of others" of the *Privacy Orientation Scale* [11]. Second, the authors individually created new items related to the target construct. Third, we requested that colleagues from our institutions participate in an online survey asking them *how they would ask people whether they value other people's privacy or not* (see [53] for a similar approach). Twelve people completed this survey; they were experts in cybersecurity and privacy, law (e.g., data privacy officers), and psychology. We also collected data from three employees of our institutes who worked in administrative roles and were not directly involved in research. Thus, we combined several sources to ensure broad and valid coverage of our construct. Moreover, our approach of item development was characterized by inclusiveness with the aim of not limiting the scope other than by construct fit. That is, rather than pre-defining different dimensions of the construct (which would also be opposed to the single-factor structure), and collecting and creating items along these lines, we chose a bottom-up approach, allowing for themes and topics to emerge that we had not considered ahead of creation. Similarly, all subsequent item elimination decisions were solely based on theoretical and statistical construct fit, rather than an attempt to cover pre-defined contexts or characteristics. The total number of items created was 87, this number is larger than twice the number of items we anticipated in our final scale (maximum 20 items), satisfying the criteria recommended by Kline and Schinka et al. [47, 73].

4.3 Refining Items

Two of the authors grouped similar items to identify common themes and removed duplicates or items that reflected a poor fit to the construct, or when their meaning was unclear (e.g., "My privacy has been violated by other people sharing my data"). We reformulated the items to be short and precise, and easily comprehensible by the target population (that is, the general public) [15, 61]. We took care to ensure that the items are non-suggestive, and require a minimal amount of subjective interpretation while responding to them [19]. After this step, 43 items remained in the item pool.

4.4 Assessing Content Validity

In the next step, we verified whether the items are relevant to and representative of the construct and whether they apply to the actual experiences of the target population. Although we applied statistical analyses to ensure the validity of the final scale (Section 6), we follow Messick's advice that evaluating the quality of the items and

how well they represent the scale construct is an ongoing process, and they should be re-evaluated after every step [58]. We started with a content validity check as recommended by Boteng et al. [15]. Assessing content validity is a form of "theoretical analysis" [59] that refers to the "adequacy with which a measure evaluates the domain of interest" [38] and is an essential step to test whether the items measure what they were supposed to measure [23]. Content validity establishes the relevance and representativeness of the items, i.e., how well the items capture the relevant experience of the target population.

Content validity should be evaluated by both domain experts and the target population [15]. Thus, we sent the revised items to two researchers in usable security and privacy, one psychology researcher (they did not participate in the first online survey described above), as well as three personal contacts of the authors outside of the research community. The items were further reformulated and four items were removed based on their suggestions. The final list included 39 items.

4.5 Pre-Testing Questions

Pre-testing helps minimize the measurement error by examining i) the extent to which the items reflect the construct being measured and ii) the extent to which the responses produce valid measurements [26]. We conducted a pilot study involving the target population and a cognitive interview study with researchers involved in scale development [15].

We assessed the extent to which the responses produce valid measurements based on how easily the items can be comprehended by the general public and how well the items represent their usual experience (i.e., their applicability). Before showing the items, we instructed our participants as follows:

> Next, you will see several statements concerning other people's privacy. Privacy means not disclosing information without the consent of the involved persons. Please indicate how strongly you disagree or agree with these statements.[1]

The study was advertised online through Prolific[2] and deployed on Qualtrics.[3] We collected data from $N = 50$ participants. However, the response from one participant was discarded because of failing the attention checks. Among the remaining 49 participants, 30 and 16 identified themselves as *female* and *male*, respectively. Fifteen participants were 25–34 years old, 13 were 35–44 years old, 12 were 18–24 years old, 6 were 45–54 years old, and 3 were 55–64 years old. About half of the participants ($n = 24$) were employed full-time, followed by students ($n = 7$) and part-time workers ($n = 6$), homemakers ($n = 4$), unemployed ($n = 4$), retired ($n = 1$), and unspecified ($n = 3$). The median completion time for the study was 4.3 minutes, and 75% of the participants completed it within 6.2 minutes. Participants were paid 1.2 USD for their time.

Participants rated the items using a 7-point Likert scale (*Strongly disagree* to *Strongly agree*). We also instructed the participants to not answer an item if it was unclear or if they have other problems answering it, and instead describe their issues in a free text space provided with each item. We also asked for their opinion and feedback on the overall study at the end of the survey. The study was approved by our institution's ethical review board.

All but one participant stated that the items were easily understandable (the exception was that one participant did not know the meaning of "CCTV"). However, two participants felt that not all items were applicable to them, e.g., "I have asked for consent before recording someone speaking" because they never recorded a conversation. Three participants discussed the context in which an item might be applicable.

Most items demonstrated wide variability across responses, but we also identified a few items that were left-skewed and had low variability. Cronbach's Alpha can only be used for one-dimensional scales. At this point, we did not calculate Cronbach's Alpha because we did not check the dimensional structure of our items yet.

We incorporated the feedback from the participants to further improve the comprehensibility and applicability of the item pool. Specifically, we removed two items and reformulated many other items. Thus, the list of items consisted of 37 items at this step.

4.5.1 Cognitive Interview. We attended a workshop on scale development and invited other attendees (both experts and novices in such research) to provide feedback regarding the construct definition, how consistently the items relate to and represent the intended construct, and the completeness of the item pool in covering all relevant aspects of the construct. Based on the feedback from a cognitive interview study, we reworded many items: for example, "I respect other people's privacy" was changed to "I respect other people's privacy without exception" to get a higher response variance, and "I protect other people's privacy even if it ruins the fun for me" was revised to "It is important to protect other people's privacy even if it ruins the fun for me" so that it reflects how much value is ascribed to the specified behavior rather than how frequently the behavior is followed through. In addition, through the discussions in this workshop, we noticed that some of our items were more appropriate to represent a criterion of the construct rather than a representation of the construct itself, since they reflected behaviors rather than values. After this step, we were left with 36 items. Among them, 15 items were designated as criterion items and were used for criterion validation (Section 6.3), and the item pool for the construct consisted of 21 items (see Table 2).

5 SCALE DEVELOPMENT

5.1 Survey Administration

The 21 items were used in an online survey ($N = 400$). We determined the sample size following Nunnally's guideline: The number of participants should be at least 10 times the number of scale items [63]. The survey was administered through Qualtrics and announced on Prolific. Participants who took part in the pilot study were excluded from participation.

[1] Prior research has cautioned against using security and privacy-related terms to avoid biasing responses because of social desirability (e.g., [24]), and the most popular approach to mitigate this issue is to use the social desirability [20] scale to control for this bias. However, recent research has questioned the scale's psychometric properties [93], and a large meta-analysis reported that the scale failed to measure the intended construct [49]. Therefore, we did not use this approach and instead relied on detecting items with skewed responses and increasing response variability by revising the items in later steps.

[2] https://www.prolific.co/

[3] https://www.qualtrics.com/

#	Item	Factor loading
1.	I don't care about other people's privacy. (r)	
2.	I respect other people's privacy without exception.*	.69
3.	I value other people's privacy more than most other people do.*	.60
4.	It is important for me to protect other people's privacy even when it is difficult to do so.*	.74
5.	Other people's privacy is valuable to me.*	.67
6.	When posting a photo with my friends online, it is important to ask for their permission first.*	.54
7.	When sharing a friends phone number on request, it is important to ask for their permission first.	
8.	When sharing information, it is important to do my best to prevent violating others' privacy.	
9.	It is important to do my best not to intrude into other people's privacy.	
10.	It is important to keep myself from looking at other people's screen notifications.*	.65
11.	It is important to look away from other people's phones when they interact with it on the bus.	.68
12.	It is okay to listen to conversations of strangers in public places.* (r)	.56
13.	It is important to protect other people's privacy even if I need to invest time and efforts to do it.*	.65
14.	It is important to protect other people's privacy even if it ruins the fun for me.*	.69
15.	It is okay to screenshot conversations from private chats and show them to others.* (r)	.62
16.	It is okay to share other's contact information (such as phone number, email) on request, even when I'm not obliged to.* (r)	.41
17.	It is okay to share photos of people who are unfamiliar to me but might be recognized by others. (r)	.52
18.	It is okay to share private information about other people without their consent. (r)	
19.	When interacting with others, it is important to respect their privacy.	
20.	When sharing pictures of tourist attractions, it is important to ensure that nobody can be clearly identified.*	.55
21.	It is important to ask for consent before recording someone speaking.*	.49

Table 2: Items after the cognitive interview. The last columns indicate the factor loading on the one-factor solution in the exploratory factor analysis (Section 5.1.2). Items marked with a star (*) are part of the final scale. Items marked with "(r)" need to be reversed before calculating the scale mean.

A majority of the participants self-identified as female (52.3%, $n = 209$), followed by male (46.0%, $n = 184$). Participants' age distribution was the following: between 18–24 (5.7%, $n = 23$), between 25–34 (22.3%, $n = 89$), between 35–44 (29.0%, $n = 116$), between 45–54 (22.0%, $n = 88$), between 55–64 (11.0%, $n = 44$), and the rest were 65 or more years old. A majority of the participants (57.0%, $n = 228$) indicated that they were employed full-time, followed by part-time workers (16.5%, $n = 66$), retired (9.3%, $n = 37$), homemakers (5.8%, $n = 23$), unemployed (5.0%, $n = 20$), other jobs (4.3%, $n = 17$) and students (2.2%, $n = 9$).

The median completion time was 5.2 minutes, and the majority of participants (75.0%, $n = 300$) completed the study within 7 minutes. We determined the response quality based on the answers to attention-check questions. Some responses (2.0%, $n = 8$) were removed because they contained incorrect answers to at least one of the attention check questions. Each participant was compensated with approximately 1.05 USD regardless of whether we used their data.

5.1.1 Item Reduction. We reassessed the validity of the pool of items based on the data from the study detailed above and removed six items. Item 1 "I don't care about other people's privacy" was removed based on a floor effect [24], it had an average value lower than 2 (on a scale ranging from 1 to 7). Five other items were removed because of the low response variance ($SD < 1$) [24]: 7. "When sharing a friend's phone number on request, it is important to ask for their permission first", 8. "When sharing information, it is important to do my best to prevent violating others' privacy", 9. "It is important to do my best not to intrude into other people's privacy", 18. "It is okay to share private information about other people without their consent", and 19. "When interacting with others, it is important to respect their privacy".

For each of the remaining items, we computed the item-total correlation, which examines the relationship between each item and the total score of all the scale items. Items with an item-total correlation less than .30 should be removed [15]; all our items had an item-total correlation above .55, and thus were retained. The internal consistency among the remaining 15 items was high (Cronbach's $\alpha = .89$ 95% CI [.87, .91]). These items were used for the exploratory factor analysis (EFA).

5.1.2 Identifying the Factor Structure. Before performing an exploratory factor analysis, we conducted *Bartlett's test of sphericity* to check whether the observed variables correlate among themselves; the result ($\chi^2 = 3433.35$, $p < .001$) indicated that our data is appropriate for factor analysis [24, 103]. Additionally, we conducted the *Kaiser-Meyer-Olkin test* (KMO) that determines the adequacy of each observed variable and the complete model. KMO values range from 0 to 1 and less than .60 is considered inadequate. We observed a KMO value of .93 [103].

To identify the number of factors to extract, we conducted a factor analysis with as many factors as items (thus, 15 factors). Using the elbow method [24, 103], we determined a one-factor structure (Figure 1). Table 2 shows the factor loading of each item.

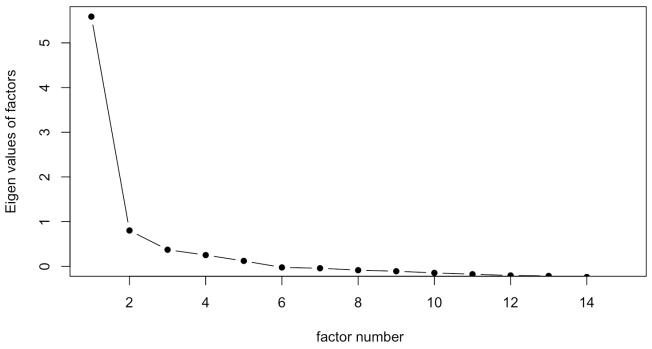

Figure 1: Scree plot to determine the appropriate number of factors.

We retained all items for the next steps since all factor loadings were above the recommended threshold of .40 [15].

5.1.3 Criterion Validity. Criterion validity can be demonstrated by measuring the extent to which scale responses predict the outcome of another related measure (usually behaviors) [23, 69]. To test the criterion validity, we let our participants answer the criteria items identified in the cognitive interview (see Section 4.5.1) after they had answered the scale items. The criteria items reflected opinions, attitudes, and behaviors related to the protection of (or putting at risk) other people's personal information. We computed means out of the 15 remaining scale items to correlate them with the criteria items. To this end, we used an ordered correlation analyses (Kendall's Tau). We note that while predictive models are usually regression-based, for exploratory research such as ours, correlation-based tests are recommended [15] and have been used in past research [24]. The proposed scale correlated highly [46] with most of the criteria items and moderately with the remaining items except one (see Table 3). The item "For safety reasons, CCTV is necessary, even when it invades other people's privacy" was not related to our scale. In the phase of pre-testing the items, one participant stated that the meaning of "CCTV" was unclear (see Section 4.5). If this was the case for multiple participants, it can explain the non-existing relationship between this criteria item and our scale. Overall, we found a strong predictive power [15] (see Table 3).

6 SCALE VALIDATION

6.1 Confirming the Factor Structure

To confirm the hypothesized factor structure extracted in the previous steps (Section 5.1.2), we conducted a test of dimensionality. Towards this goal, we administered another online study using the 15 items that remained in the previous step. As before, we implemented the study in Qualtrics and promoted it in Prolific; previous participants were not allowed to participate in the study, ensuring the independence of samples from previous studies [15].

Survey questionnaires. To investigate how closely our scale is related to other measures of similar constructs (convergent validity) and whether our scale is unrelated to constructs different from our domain of interest (discriminant validity), we included three other questionnaires in the study. The first survey we included was the unidimensional *Privacy Concern Scale* developed by Buchanan et al. [18], which constitutes of 16 questions asking about one's concern about self-privacy (e.g., "In general, how concerned are you about your privacy while you are using the internet?"). Next, we included the *Self- and Other-Interest Inventory* by Gerbasi and Prentice [28]; it included eight items related to activities that advance self-interests (e.g., "I am constantly looking for ways to get ahead") and another eight items related to activities toward others' interest (e.g., "I keep an eye out for others' interests"). We also included five items from Baruh et al.'s *Concern about privacy of others* sub-scale that was part of the *Privacy Orientation Scale* (an example item is "I always do my best not to intrude into other people's private lives") [11]. To investigate how our measure relates to the 10 basic human values, we included the short questionnaire created by Lindeman and Verkasalo that asks *how much importance one ascribes to each of the 10 basic values* [50]; the response scale ranged from "Opposed to my principle" to "Extremely important". Questionnaires from these scales were organized in blocks; the order of the blocks, as well as the questions within the blocks, were randomized.

Participants. We collected data from 1,000 participants on Prolific. 51.4% (n = 514) and 46.8% (n = 468) of the participants self-identified as male and female, respectively. Participants' age distribution showed the following: between 18–24 (5.8%, n = 58), between 25–34 (28.2%, n = 282), between 35–44 (28.6%, n = 286), between 45–54 (16.0%, n = 160), between 55–64 (14.6%, n = 146), and the rest were 65 or more years old. A majority of the participants indicated that they were employed full-time (61.8%, n = 618), followed by part-time workers (14.9%, n = 149), retired (6.9%, n = 69), unemployed (7.7%, n = 77), homemakers (4.3%, n = 43), other jobs (3.7%, n = 37) and students (1.1%, n = 11). We removed responses (13.5%, n = 135), incorrectly answering the attention check questions or with a high inter-item standard deviation (ISD) [10]. The ISD is a measure recommended by Barends and Vries [10] to identify random responses in a survey. The median completion time was 8 minutes, and the majority of participants (75%, n = 750) completed the study within 11 minutes. Each participant was compensated with approximately 2.1 USD regardless of whether we used their data.

Confirmatory factor analysis. We performed an (ordinal) confirmatory factor analysis with the collected data [15]. We report the following fit indices: the Root Mean Square Error of Approximation (RMSEA), the Standardized Root Mean Square Residual (SRMR), the Comparative Fit Index (CFI), and the Tucker-Lewis Index (TLI) [15], but omit the chi-square goodness-of-fit test (which is unreliable for a large sample size [41, 82, 94]). Both CFI and TLI were above .99, indicating exceptional fit [15]. The RMSEA was .085, slightly above the recommended value of .08 for an adequate fit [41], and SRMR was .052, indicating a good fit (values above .06 suggest a poor fit). To improve RMSEA, we performed a standard model selection procedure as explained below.

Model selection. Model selection is frequently used in structural equation modeling to identify the 'optimal' model based on some selection criteria such as Akaike information criterion (AIC), Bayesian

Criterion item	r_τ	95% CI
A crime needs to be serious to justify a search warrant for someone's phone.	.22	[.15, .28]
Care should be taken when disclosing information about other people.	.45	[.40, .50]
Everyone has a right to keep their information private.	.36	[.30, .42]
For safety reasons, CCTV is necessary, even when it invades other people's privacy.	.03	[-.04, .09]
I don't like that some apps on my smartphone require access to my contacts.	.30	[.24, .36]
Most of the time when using technologies, it is unavoidable to violate someone's privacy.	.24	[.18, .30]
Other people's need for privacy should be considered when disclosing information about them.	.47	[.41, .52]
People using wearable cameras in public places put other people's privacy at risk.	.31	[.25, .37]
Sharing pictures of babies does not need the consent of their parents even when it is required by law.	.29	[.23, .35]
When other people give me their phone number, I can use it for any purpose.	.41	[.35, .46]
When someone shares their picture, they have lost their right to keep it private.	.25	[.19, .31]
I own information I obtain about others.	.30	[.23, .35]
I have been accused of violating someone else's privacy.	.34	[.28, .40]
People have been angry at me, because I have shared their information without consent.	.31	[.25, .37]
I have asked people for permission before taking their photograph.	.39	[.33, .44]

Table 3: Correlation (Kendall's Tau) between the scale and criteria items suggests the scale's ability to predict opinions and related behaviors. $.20 \geq r_\tau < .30$ **and** $r_\tau \geq .30$ **indicate moderate and high correlation, respectively [46].**

information criterion (BIC) and RMSEA [96]. We followed a step-wise model selection procedure analogous to step-wise regression with backward elimination: at each step, we compared the current best model (i.e., minimal RMSEA) with models created by removing a single item [42, 96]. More precisely, first, we compare the full model with models that contained one item less. Next, we compare the best model identified in the previous step with models that can be created by removing other items. This process continues until the RMSEA cannot be further improved [96]. We found that removing items 11 and 17 (Table 2) from the model specification resulted in a 'close fit' model [15, 41] according to all fit indices ($RMSEA = .05, CFI > .99, TLI > .99$). Thus, our final scale contains 13 items (see Appendix A).

6.2 Test of Reliability

Using the data from the above sample, we investigated the reliability of our measurement. Reliability indicates the consistency between items' repeated use under identical conditions [15]. The consistency score measured through Cronbach's α for the 13 items was .92 95% CI [.91, .93], well above the requirement of .70 [15]. We also report the ordinal Alpha (i.e., ordinal version of Cronbach's Alpha [105]) of .94 95% CI [.87, .98]. The composite reliability [47] score was .94 (well above the recommended threshold of .60 [7]).

6.3 Tests of Validity

Scale validity refers to the extent to which the scale measures the construct that it was developed to measure [69]. The most common tests of validity include *content* (assessed in Step 2), *criterion*, and *construct validity* [15]. The tested criterion validity was already reported in Section 5.1.3.

6.3.1 Construct Validity. We assessed construct validity through convergent and discriminant analyses [15]. For convergent validity, we first looked at the *Other-Interest* subscale (as part of the Self-Other-Interest-Inventory) proposed by Gerbasi and Prentice [28], which measures one's motivation to act in other people's interest. The sub-scale demonstrated a high internal consistency for our sample (Cronbach's $\alpha = .88$). We hypothesized a positive relationship between our scale and that subscale because the motivation to act in another person's interest and the importance to protect their privacy should share conceptual overlap. Our scale demonstrated a significant positive correlation ($r_\tau = .21, p < .001$) with a medium effect size [46] with the *Other-Interest* scale. Additionally, we tested whether our scale is related to existing scales measuring concern for others' privacy. We calculated the correlation between the 5-item sub-scale *Concern about the privacy of others* by Baruh et al. [11]) and the value of others' privacy. The scale also demonstrated a high internal consistency (Cronbach's $\alpha = .89$ for our sample) and correlated significantly with our scale ($r_\tau = .50, p < .001$). In other words, 25.0% of the response variance in our scale can be explained by concern for other people's privacy (or vice versa). Unsurprisingly, as these two measures assess similar constructs (and we adapted two items from this sub-scale in our item pool), they share substantial conceptual overlap. Yet, these results also indicate that our scale is sufficiently distinct from measuring concern for others' privacy, as 75.0% of the total variance cannot be explained by concerns about the privacy of others (or vice versa).

To determine discriminant validity, we calculated the correlation between our scale and the *Self-Interest* subscale [28], which measures one's motivation to act in self-interest and demonstrated a high internal consistency for our sample (Cronbach's $\alpha = .91$). Since the protection of other people's privacy is a socially-focused behavior, we expected that our scale will not have any systematic relation with the *Self-Interest* scale and the result ($r_\tau = -.02, p > .5$) substantiated our hypothesis. Please note that we published the correlations of our individual items with the Basic Human Values and the Self-/Other-Interest scales at https://osf.io/q5y4d/wiki/Item%20Correlations/.

We further tested whether the value of others' privacy is distinct from (but related to) being concerned about own privacy. To this

end, we used the *Privacy Concern Scale* by Buchanan et al. [18], which demonstrated high internal reliability (Cronbach's $\alpha = .94$ for our sample). The relation between self-privacy concern and the value of others' privacy was positive and significant ($r_\tau = .18$, $p < .001$), indicating that, while the majority of variation (i.e., 96.8%) in our scale cannot be explained by concern for self-privacy (or vice versa), both scales, not surprisingly, share some conceptual overlap. That is, the value of others' privacy is not independent of self-privacy concerns.

6.4 Relationship Between Our Scale and the Fundamental Human Values

To examine how the value of others' privacy relates to the 10 fundamental human values [75], we used the questionnaire by Lindeman and Verkasalo [50] that asks how much importance one ascribes to each of the 10 fundamental values. We found that "value of other people's privacy" correlates with *self-direction* ($r_\tau = .26$), *universalism* ($r_\tau = .25$), *benevolence* ($r_\tau = .31$), *tradition* ($r_\tau = .12$), *conformity* ($r_\tau = .15$), and *security* ($r_\tau = .20$), all ps $< .001$; but did not correlate with *power* ($r_\tau = -.09$), *achievement* ($r_\tau = .07$), *hedonism* ($r_\tau = .01$), or *stimulation* ($r_\tau = .06$). Thus, in line with our expectation, our scale correlates with all values that are socially-focused and does not correlate with most personal-focused values. Interestingly, "value of other people's privacy" correlates with self-direction, which is broadly defined as independent thought and action [76]. At this point, we can only speculate that people who exhibit a high value of other people's privacy, might perceive the impact that protecting other's privacy has on their own independence as low, or they might perceive the protection of other's privacy as a free non-mandatory choice, which aligns with their high value of self-direction. Future research should address this question.

7 DISCUSSIONS AND LIMITATIONS

We developed a psychometric scale to measure how much an individual ascribes importance to protect a data subject's privacy. Our methods followed the best practices recommended by the extant literature for scale development [e.g., 15, 61]; and we refined the construct definition and the indicator items in multiple rounds based on experts' feedback and three studies. The resulting unidimensional scale demonstrated desirable psychometric properties such as high internal consistency, reliability, fit indices for the factor structure, and convergent and discriminant validity. Notably, the uni-dimensionality of the scale suggests that response behavior to all items was driven by the assumed underlying construct: the value of other people's privacy. Moreover, our target construct relates back to the basic human values that were proposed to underlie actions and behaviors; as evidenced in the correlations of our scale with the basic values that motivate behavior in the interest of other people rather than in the interest of the self. Drawing on these connections, the proposed scale will allow us to leverage the rich extant literature on how values motivate intentions and actions to predict expected behaviors in interdependent privacy settings [9, 90].

The *value of other people's privacy* scale (or *VOPP* in short) can benefit researchers studying human-computer interactions and human factors in privacy and security. Since people's adoption of technology and how they interact with them are among the primary focus within the HCI community, quantifying the potential users' consideration of privacy risks to others can provide new insights into the adoption and use of a certain technology. Additionally, predicting behaviors can aid designing interactions in privacy-preserving ways. Similarly, usable privacy and security researchers can leverage this scale to design PETs and interventions that suit the users. For example, persuasive interventions can be designed for users who exhibit a relatively low value of other people's privacy to encourage them in privacy-protective behaviors. Contrarily, people who exhibit a higher value of other people's privacy might be more open to a more privacy-preserving version of the technology that may require more technical knowledge to use. Finally, even though values are assumed to be relatively stable over time and situations, certain ways how values can be changed have been identified [8]. Thus, future research might be able to devise interventions to enhance the value of other people's privacy, allowing building systems that are more privacy-protecting, which in turn are more likely to be adopted by users.

7.1 Limitations

Our data and, consequently, results may suffer from selection bias as we collected data only from a U.S.-based population. More research is needed to evaluate the reliability and validity of our measurements in other cultures. Further selection bias might have been introduced by our mode of data collection (i.e., through online surveys) from a non-random population, although recent research has reported that Prolific appears to be better at representing the US population than other alternatives for studies related to privacy perceptions [89].

Our approach to item development entailed not pre-defining the scope (other than construct-fit) with respect to, for instance, type of information (e.g., images), specific behaviors (e.g., physical sharing), contexts (e.g., social media) or recipient characteristics (e.g., friends) for the items, to allow for an emergence of topics and themes we had not considered before. As a result, all items reflect the general value of privacy of others but vary in their level of abstractness, with some items addressing concrete scenarios while other items being rather abstract. Thus, the question arises whether our scale is comprehensive, in the sense that it neither covers a wide range of interdependent privacy scenarios exhaustively nor could the sum of items be described as entirely context-independent. We are confident that our scale is suitable to assess the value of privacy of others above and beyond the contexts depicted in our items because response behavior on each item is driven by the same underlying construct. Our statistical analyses show that items are highly related to each other. Accordingly, we conclude that the construct of interest has a stronger influence on responses to the items compared to the specific contexts depicted by the items.

8 FUTURE WORK

The newly developed scale is a foundational measure to explain people's behavior and their interaction with existing and emerging technologies. This scale will be increasingly relevant to understanding and predicting users' behaviors as we get surrounded by IoT devices and wearable sensors that collect multimodal data about

everyone around, vehicles and drones equipped with cameras and other sensors become commonplace, and smart and connected cities become the reality. Additionally, this scale will allow studying and comparing subpopulations with different demographics (age, gender, etc.) and cultures, as these factors might influence people's response to technology. For example, cultural background may influence the importance people ascribe to other people's privacy, which may in turn dictate their technology adoption. Furthermore, since our scale is not specific to a certain technology, it can be applied to technologies that are not yet developed or even conceived.

Another avenue for future research is the investigation of other factors and contexts that might interact with the value of other people's privacy and can be manipulated independently of the scale measure. For example, the impact of value might vary depending on the type of data being shared (e.g., health data vs. email address), with a greater impact on (subjectively) more sensitive data. It might also vary from one context to another with less impact on (subjectively) more public contexts (e.g., an image of a bystander on a crowded street vs. a lonely forest) or contexts that are interpreted as licensing privacy breaches (e.g., delinquent behavior). Particularly interesting might be the investigation of different types of social relations (e.g., family members, friends, strangers) another person can have with an individual. On the one hand, it can be hypothesized that the impact of the value of other people's privacy should be greater for socially close persons because the likelihood of prosocial behavior is higher [64]. On the other hand, it might be hypothesized that the impact is lower as socially close persons might be more likely to forgive a privacy breach [45]. We plan to build a *causal* model that includes other relevant variables (e.g., risk awareness, possible receivers of information), and empirically validate it with real-world behavioral data that we will collect through custom mobile apps and browser plugins and additionally manipulate other factors, like the ones mentioned above that might act as moderators for the value of other people's privacy.

The assumption that our scale measures a cross-contextual, basic, and more stable construct compared to *privacy concern* and *privacy attitude* is based on theoretical grounds. We plan to provide empirical evidence for this claim in future studies. More specifically, we plan to experimentally demonstrate that varying related factors, such as risk awareness and technical skills, will change individuals' *concern for other people's privacy*, but their *value of other people's privacy* will remain unaffected.

In addition, we propose a closer investigation of situations in which values conflict with each other [76]. More specifically, the value of privacy might contradict the value of security and hedonism. For example, a location tracking system at the workplace can be privacy-threatening but might foster an individual's security in the case of an emergency. Moreover, not publishing a video on social media and thus, not receiving any positive feedback from others, to protect the privacy of bystanders, might interfere with the hedonism of an individual. Thus, to better understand the role of the value of other people's privacy in the face of other conflicting values, we will investigate the relative importance of the value and its predictive power in different contexts.

9 CONCLUSION

Concern for self-privacy has been recognized as a prime factor in technology's adoption and use, and significant research efforts have been dedicated to measuring and mitigating those concerns. The use of technology, however, also risks the privacy of a vast number of non-users; but whether and how the users consider other people's privacy remained under-studied. This paper lays a foundation for future research by proposing a theoretically grounded construct and empirically validating a scale to measure it. The scale demonstrated high internal consistency, and convergent and discriminant validity. We are confident that the proposed scale is useful for studying numerous interdependent privacy contexts, providing the opportunity to understand and mitigate privacy issues raised by existing and emerging technologies.

ACKNOWLEDGMENTS

We are grateful to our colleagues at Arizona State University, CISPA Helmholtz Center for Information Security, and other institutes for their participation and helpful suggestions in various stages of the scale development process. We thank all the study participants for their time and efforts.

REFERENCES

[1] Paarijaat Aditya, Rijurekha Sen, Peter Druschel, Seong Joon Oh, Rodrigo Benenson, Mario Fritz, Bernt Schiele, Bobby Bhattacharjee, and Tong Tong Wu. 2016. I-pic: A platform for privacy-compliant image capture. In *Proceedings of the 14th annual international conference on mobile systems, applications, and services (MobiSys '16)*. ACM, New York, NY, USA, 235–248. https://doi.org/10.1145/2906388.2906412

[2] Icek Ajzen. 2012. Values, Attitudes, and Behavior. In *Methods, Theories, and Empirical Applications in the Social Sciences*, Samuel Salzborn, Eldad Davidov, and Jost Reinecke (Eds.). VS Verlag für Sozialwissenschaften, Wiesbaden, 33–38. https://doi.org/10.1007/978-3-531-18898-0_5

[3] Mary Jean Amon, Rakibul Hasan, Kurt Hugenberg, Bennett I Bertenthal, and Apu Kapadia. 2020. Influencing photo sharing decisions on social media: A case of paradoxical findings. In *the proceedings of the IEEE symposium on security & privacy (SP '20)*. IEEE Computer Society, San Francisco, CA, USA, 1350–1366. https://doi.org/10.1109/SP40000.2020.00006

[4] Mark Andrejevic and Neil Selwyn. 2020. Facial recognition technology and the end of privacy for good. https://lens.monash.edu/2020/01/23/1379547/facial-recognition-tech-and-the-end-of-privacy

[5] Erman Ayday, Emiliano De Cristofaro, Jean-Pierre Hubaux, and Gene Tsudik. 2015. Whole Genome Sequencing: Revolutionary Medicine or Privacy Nightmare? *Computer* 48, 2 (Feb. 2015), 58–66. https://doi.org/10.1109/MC.2015.59

[6] Erman Ayday and Mathias Humbert. 2017. Inference Attacks against Kin Genomic Privacy. *IEEE Security & Privacy* 15, 5 (2017), 29–37. https://doi.org/10.1109/MSP.2017.3681052

[7] Richard P. Bagozzi and Youjae Yi. 1988. On the evaluation of structural equation models. *Journal of the Academy of Marketing Science* 16, 1 (March 1988), 74–94. https://doi.org/10.1007/BF02723327

[8] Anat Bardi and Robin Goodwin. 2011. The dual route to value change: Individual processes and cultural moderators. *Journal of cross-cultural psychology* 42, 2 (2011), 271–287.

[9] Anat Bardi and Shalom H. Schwartz. 2003. Values and Behavior: Strength and Structure of Relations. *Personality and Social Psychology Bulletin* 29, 10 (Oct. 2003), 1207–1220. https://doi.org/10.1177/0146167203254602

[10] Ard J. Barends and Reinout E. de Vries. 2019. Noncompliant responding: Comparing exclusion criteria in MTurk personality research to improve data quality. *Personality and Individual Differences* 143 (June 2019), 84–89. https://doi.org/10.1016/j.paid.2019.02.015

[11] Lemi Baruh and Zeynep Cemalcılar. 2014. It is more than personal: Development and validation of a multidimensional privacy orientation scale. *Personality and Individual Differences* 70 (2014), 165–170. https://doi.org/10.1016/j.paid.2014.06.042

[12] Julia Bernd, Ruba Abu-Salma, Junghyun Choy, and Alisa Frik. 2022. Balancing power dynamics in smart homes: Nannies' perspectives on how cameras reflect and affect relationships. In *Eighteenth symposium on usable privacy and security (SOUPS 2022)*. USENIX Association, Boston, MA, 687–706. https://www.usenix.

org/conference/soups2022/presentation/bernd
[13] Julia Bernd, Ruba Abu-Salma, and Alisa Frik. 2020. Bystanders privacy: The perspectives of nannies on smart home surveillance. In *10th USENIX workshop on free and open communications on the internet (FOCI 20)*. USENIX Association. https://www.usenix.org/conference/foci20/presentation/bernd
[14] Gergely Biczók and Pern Hui Chia. 2013. Interdependent privacy: Let me share your data. In *International conference on financial cryptography and data security*, Ahmad-Reza Sadeghi (Ed.). Springer, Berlin, 338–353.
[15] Godfred O. Boateng, Torsten B. Neilands, Edward A. Frongillo, Hugo R. Melgar-Quiñonez, and Sera L. Young. 2018. Best Practices for Developing and Validating Scales for Health, Social, and Behavioral Research: A Primer. *Frontiers in Public Health* 6 (June 2018), 149. https://doi.org/10.3389/fpubh.2018.00149
[16] Thomas Brewster. 2022. A "Threat To Black Communities": Senators Call On Immigration Cops And FBI To Quit Using Clearview Facial Recognition. https://www.forbes.com/sites/thomasbrewster/2022/02/09/a-threat-to-black-communities-senators-call-on-immigration-cops-and-fbi-to-quit-using-clearview-facial-recognition/
[17] Tom Buchanan, Carina Paine, Adam N. Joinson, and Ulf-Dietrich Reips. 2007. Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology* 58, 2 (Jan. 2007), 157–165. https://doi.org/10.1002/asi.20459
[18] Tom Buchanan, Carina Paine, Adam N. Joinson, and Ulf-Dietrich Reips. 2007. Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology* 58, 2 (2007), 157–165. https://doi.org/10.1002/asi.20459 tex.eprint: https://asistdl.onlinelibrary.wiley.com/doi/pdf/10.1002/asi.20459.
[19] Jessica Colnago, Lorrie Faith Cranor, Alessandro Acquisti, and Kate Hazel Jain. 2022. 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)*. USENIX Association, Boston, MA, 331–346. https://www.usenix.org/conference/soups2022/presentation/colnago
[20] Douglas P Crowne and David Marlowe. 1960. A new scale of social desirability independent of psychopathology. *Journal of consulting psychology* 24, 4 (1960), 349. Publisher: American Psychological Association.
[21] Anupam Das, Martin Degeling, Daniel Smullen, and Norman Sadeh. 2018. Personalized Privacy Assistants for the Internet of Things: Providing Users with Notice and Choice. *IEEE Pervasive Computing* 17, 3 (July 2018), 35–46. https://doi.org/10.1109/MPRV.2018.03367733
[22] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. 2014. In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies. In *Proceedings of the 32Nd annual ACM conference on human factors in computing systems (CHI '14)*. ACM, New York, NY, USA, 2377–2386. https://doi.org/10.1145/2556288.2557352
[23] Robert F DeVellis and Carolyn T Thorpe. 2021. *Scale development: Theory and applications*. Sage publications.
[24] Serge Egelman and Eyal Peer. 2015. Scaling the security wall: Developing a security behavior intentions scale (SeBIS). In *Proceedings of the 33rd annual ACM conference on human factors in computing systems (CHI '15)*. Association for Computing Machinery, New York, NY, USA, 2873–2882. https://doi.org/10.1145/2702123.2702249
[25] Cori Faklaris, Laura A. Dabbish, and Jason I. Hong. 2019. A Self-Report measure of End-User security attitudes (SA-6). In *Fifteenth symposium on usable privacy and security (SOUPS 2019)*. USENIX Association, Santa Clara, CA, 61–77. https://www.usenix.org/conference/soups2019/presentation/faklaris
[26] Floyd J Fowler Jr and Floyd J Fowler. 1995. *Improving survey questions: Design and evaluation*. Sage.
[27] Christine Geeng and Franziska Roesner. 2019. Who's in control? Interactions in multi-user smart homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–13.
[28] Margaret E. Gerbasi and Deborah A. Prentice. 2013. The Self- and Other-Interest Inventory. *Journal of Personality and Social Psychology* 105, 3 (2013), 495–514. https://doi.org/10.1037/a0033483
[29] Nina Gerber, Paul Gerber, and Melanie Volkamer. 2018. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & security* 77 (2018), 226–261.
[30] Thomas Groß. 2021. Validity and reliability of the scale internet users' information privacy concerns (iuipc). *Proceedings on Privacy Enhancing Technologies* (2021). Publisher: Newcastle University.
[31] Edward T Hall, Ray L Birdwhistell, Bernhard Bock, Paul Bohannan, A Richard Diebold Jr, Marshall Durbin, Munro S Edmonson, JL Fischer, Dell Hymes, Solon T Kimball, et al. 1968. Proxemics [and comments and replies]. *Current anthropology* 9, 2/3 (1968), 83–108.
[32] Rakibul Hasan, Bennett I Bertenthal, Kurt Hugenberg, and Apu Kapadia. 2021. Your photo is so funny that I don't mind violating your privacy by sharing it: Effects of individual humor styles on online photo-sharing behaviors. In *Proceedings of the 2021 CHI conference on human factors in computing systems (CHI'21)*. ACM. https://doi.org/10.1145/3411764.3445258
[33] Rakibul Hasan, David Crandall, and Mario Fritz Apu Kapadia. 2020. Automatically detecting bystanders in photos to reduce privacy risks. In *2020 IEEE symposium on security and privacy (SP)*. IEEE Computer Society, Los Alamitos, CA, USA.
[34] Rakibul Hasan, Eman Hassan, Yifang Li, Kelly Caine, David J Crandall, Roberto Hoyle, and Apu Kapadia. 2018. Viewer experience of obscuring scene elements in photos to enhance privacy. In *Proceedings of the 2018 CHI conference on human factors in computing systems (CHI '18)*. ACM, New York, NY, USA, 47:1–47:13. https://doi.org/10.1145/3173574.3173621
[35] Rakibul Hasan, Yifang Li, Eman Hassan, Kelly Caine, David J. Crandall, Roberto Hoyle, and Apu Kapadia. 2019. Can privacy be satisfying? On improving viewer satisfaction for privacy-enhanced photos using aesthetic transforms. In *Proceedings of the 2019 CHI conference on human factors in computing systems*, Vol. 14. ACM, 25. https://doi.org/10.1145/3290605.3300597
[36] Stephen N. Haynes, David C. S. Richard, and Edward S. Kubany. 1995. Content validity in psychological assessment: A functional approach to concepts and methods. *Psychological Assessment* 7, 3 (Sept. 1995), 238–247. https://doi.org/10.1037/1040-3590.7.3.238
[37] Kashmir Hill. 2020. The secretive company that might end privacy as we know it. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html
[38] Timothy R. Hinkin. 1995. A Review of Scale Development Practices in the Study of Organizations. *Journal of Management* 21, 5 (Oct. 1995), 967–988. https://doi.org/10.1177/014920639502100509
[39] Timothy R. Hinkin. 1998. A brief tutorial on the development of measures for use in survey questionnaires. *Organizational Research Methods* 1, 1 (1998), 104–121. https://doi.org/10.1177/109442819800100106 tex.readstatus: skimmed.
[40] Roberto Hoyle, Robert Templeman, Steven Armes, Denise Anthony, David Crandall, and Apu Kapadia. 2014. Privacy behaviors of lifeloggers using wearable cameras. In *Proceedings of the 2014 ACM international joint conference on pervasive and ubiquitous computing (UbiComp '14)*. ACM, New York, NY, USA, 571–582. https://doi.org/10.1145/2632048.2632079
[41] Li-tze Hu and Peter M. Bentler. 1999. Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal* 6, 1 (Jan. 1999), 1–55. https://doi.org/10.1080/10705519909540118
[42] Po-Hsien Huang. 2017. Asymptotics of AIC, BIC, and RMSEA for Model Selection in Structural Equation Modeling. *Psychometrika* 82, 2 (June 2017), 407–426. https://doi.org/10.1007/s11336-017-9572-y
[43] Yue Huang, Borke Obada-Obieh, and Konstantin Beznosov. 2020. Amazon vs. my brother: How users of shared smart speakers perceive and cope with privacy risks. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–13.
[44] Mathias Humbert, Benjamin Trubert, and Kévin Huguenin. 2019. A survey on interdependent privacy. *Acm Computing Surveys* 52, 6 (Oct. 2019). https://doi.org/10.1145/3360498 Place: New York, NY, USA Publisher: Association for Computing Machinery.
[45] Johan C Karremans, Camillo Regalia, F Giorgia Paleari, Frank D Fincham, Ming Cui, Naomi Takada, Ken-Ichi Ohbuchi, Kari Terzino, Susan E Cross, and Ayse K Uskul. 2011. Maintaining harmony across the globe: The cross-cultural association between closeness and interpersonal forgiveness. *Social Psychological and Personality Science* 2, 5 (2011), 443–451.
[46] M.G. Kendall. 1948. *Rank correlation methods*. Griffin, Oxford, England.
[47] Paul Kline. 2013. *Handbook of psychological testing*. Routledge.
[48] Mehrdad Koohikamali, Daniel A Peak, and Victor R Prybutok. 2017. Beyond self-disclosure: Disclosure of information about others in social network sites. *Computers in Human Behavior* 69 (2017), 29–42. https://doi.org/10.1016/j.chb.2016.12.012
[49] Lukas Lanz, Isabel Thielmann, and Fabiola H. Gerpott. 2022. Are social desirability scales desirable? A meta-analytic test of the validity of social desirability scales in the context of prosocial behavior. *Journal of Personality* 90, 2 (April 2022), 203–221. https://doi.org/10.1111/jopy.12662
[50] Marjaana Lindeman and Markku Verkasalo. 2005. Measuring Values With the Short Schwartz's Value Survey. *Journal of Personality Assessment* 85, 2 (Oct. 2005), 170–178. https://doi.org/10.1207/s15327752jpa8502_09
[51] Ring LLC. 2022. Uploading images, photos, or videos to the Neighbors app. https://support.ring.com/hc/en-us/articles/360050968372-Uploading-images-photos-or-videos-to-the-Neighbors-app
[52] Gregory R Maio and James M Olson. 2000. What is a "value-expressive" attitude. *Why we evaluate: Functions of attitudes* 249269 (2000).
[53] Naresh K Malhotra, Sung S Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research* 15, 4 (2004), 336–355. https://doi.org/10.1287/isre.1040.0032
[54] Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. 2020. Smart Devices in Airbnbs: Considering Privacy and Security for both Guests and Hosts. *Proc. Priv. Enhancing Technol.* 2020, 2 (2020), 436–458.

[55] Karola Marky, Alexandra Voit, Alina Stöver, Kai Kunze, Svenja Schröder, and Max Mühlhäuser. 2020. " I don't know how to protect myself": Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*. 1–11.

[56] Maximilian Marsch, Jens Grossklags, and Sameer Patil. 2021. Won't You Think of Others?: Interdependent Privacy in Smartphone App Permissions. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (Oct. 2021), 1–35. https://doi.org/10.1145/3479581

[57] D Betsy McCoach, Robert K Gable, and John P Madura. 2013. *Instrument development in the affective domain*. Vol. 10. Springer.

[58] Samuel Messick. 1995. Validity of psychological assessment: Validation of inferences from persons' responses and performances as scientific inquiry into score meaning. *American Psychologist* 50, 9 (Sept. 1995), 741–749. https://doi.org/10.1037/0003-066X.50.9.741

[59] Fabiane F. R. Morgado, Juliana F. F. Meireles, Clara M. Neves, Ana C. S. Amaral, and Maria E. C. Ferreira. 2017. Scale development. Ten main limitations and recommendations to improve future research practices. *Psicologia: Reflexão e Crítica* 30, 1 (Jan. 2017). https://doi.org/10.1186/s41155-016-0057-1 Publisher: Springer Science and Business Media LLC tex.owner: siegel.

[60] Joshua Morris, Sara Newman, Kannappan Palaniappan, Jianping Fan, and Dan Lin. 2021. "Do You Know You Are Tracked by Photos That You Didnt Take: Large-Scale Location-Aware Multi-Party Image Privacy Protection. *IEEE Transactions on Dependable and Secure Computing* (2021), 1–1. https://doi.org/10.1109/TDSC.2021.3132230

[61] Richard G Netemeyer, William O Bearden, and Subhash Sharma. 2003. *Scaling procedures: Issues and applications*. sage publications.

[62] ALFRED NG. 2022. Amazon gave Ring videos to police without owners' permission. https://www.politico.com/news/2022/07/13/amazon-gave-ring-videos-to-police-without-owners-permission-00045513

[63] Jum C Nunnally. 1967. Psychometric theory. (1967). Publisher: McGraw-hill.

[64] Thomas O Passarelli and Tony W Buchanan. 2020. How do stress and social closeness impact prosocial behavior? *Experimental Psychology* 67, 2 (2020), 123.

[65] Björn N. Persson and Petri J. Kajonius. 2016. Empathy and universal values explicated by the empathy-altruism hypothesis. *The Journal of Social Psychology* 156, 6 (Nov. 2016), 610–619. https://doi.org/10.1080/00224545.2016.1152212

[66] Yu Pu and Jens Grossklags. 2015. Using conjoint analysis to investigate the value of interdependent privacy in social app adoption scenarios. *Proceedings of the International Conference on Information Systems (ICIS 2015)* (2015).

[67] Yu Pu and Jens Grossklags. 2016. Towards a model on the factors influencing social app users' valuation of interdependent privacy. *Proceedings on Privacy Enhancing Technologies* 2016, 2 (2016), 61–81. https://doi.org/10.1515/popets-2016-0005 Place: Berlin Publisher: Sciendo.

[68] Yasmeen Rashidi, Apu Kapadia, Christena Nippert-Eng, and Norman Makoto Su. 2020. "It's easier than causing confrontation": Sanctioning strategies to maintain social norms of content sharing and privacy on social media. *To appear in the Proceedings of the ACM Journal: Human-Computer Interaction: Computer Supported Cooperative Work and Social Computing (CSCW '20)* (2020).

[69] Tenko Raykov and George A Marcoulides. 2011. *Introduction to psychometric theory*. Routledge.

[70] Robert J Rydell and Bertram Gawronski. 2009. I like you, I like you not: Understanding the formation of context-dependent automatic attitudes. *Cognition and Emotion* 23, 6 (2009), 1118–1152. Publisher: Taylor & Francis.

[71] Lilach Sagiv, Sonia Roccas, Jan Cieciuch, and Shalom H. Schwartz. 2017. Personal values in human life. *Nature Human Behaviour* 1, 9 (Sept. 2017), 630–639. https://doi.org/10.1038/s41562-017-0185-3 tex.copyright: 2017 The Author(s).

[72] Kavous Salehzadeh Niksirat, Evanne Anthoine-Milhomme, Samuel Randin, Kévin Huguenin, and Mauro Cherubini. 2021. "I thought you were okay": Participatory Design with Young Adults to Fight Multiparty Privacy Conflicts in Online Social Networks. In *Designing Interactive Systems Conference 2021*. 104–124.

[73] John A Schinka, Wayne F Velicer, Alice F Healy, Robert W Proctor, Walter C Borman, Daniel R Ilgen, and Richard J Klimoski. 2003. *Handbook of psychology, developmental psychology*. Vol. 6. John Wiley & Sons.

[74] P Wesley Schultz, Valdiney V Gouveia, Linda D Cameron, Geetika Tankha, Peter Schmuck, and Marek Franěk. 2005. Values and their relationship to environmental concern and conservation behavior. *Journal of cross-cultural psychology* 36, 4 (2005), 457–475. Publisher: Sage Publications Sage CA: Thousand Oaks, CA.

[75] Shalom H. Schwartz. 1992. Universals in the Content and Structure of Values: Theoretical Advances and Empirical Tests in 20 Countries. In *Advances in Experimental Social Psychology*. Vol. 25. Academic Press, 1–65. https://doi.org/10.1016/S0065-2601(08)60281-6

[76] Shalom H Schwartz. 2012. An overview of the Schwartz theory of basic values. *Online readings in Psychology and Culture* 2, 1 (2012), 2307–0919.

[77] Shalom H. Schwartz, Jan Cieciuch, Michele Vecchione, Eldad Davidov, Ronald Fischer, Constanze Beierlein, Alice Ramos, Markku Verkasalo, Jan-Erik Lönnqvist, Kursad Demirutku, Ozlem Dirilen-Gumus, and Mark Konty. 2012. Refining the theory of basic individual values. *Journal of Personality and Social Psychology* 103, 4 (Oct. 2012), 663–688. https://doi.org/10.1037/a0029393

[78] Shalom H Schwartz and Judith A Howard. 1981. A normative decision-making model of altruism. *Altruism and helping behavior* (1981), 189–211.

[79] Shalom H. Schwartz and Judith A. Howard. 1984. Internalized Values as Motivators of Altruism. In *Development and Maintenance of Prosocial Behavior*, Ervin Staub, Daniel Bar-Tal, Jerzy Karylowski, and Janusz Reykowski (Eds.). Springer US, Boston, MA, 229–255. https://doi.org/10.1007/978-1-4613-2645-8_14

[80] Shalom H. Schwartz and Tammy Rubel. 2005. Sex differences in value priorities: Cross-cultural and multimethod studies. *Journal of Personality and Social Psychology* 89, 6 (Dec. 2005), 1010–1028. https://doi.org/10.1037/0022-3514.89.6.1010

[81] Dzemila Sero, Arslan Zaidi, Jiarui Li, Julie D. White, Tomás B. González Zarzar, Mary L. Marazita, Seth M. Weinberg, Paul Suetens, Dirk Vandermeulen, Jennifer K. Wagner, Mark D. Shriver, and Peter Claes. 2019. Facial recognition from DNA using face-to-DNA classifiers. *Nature Communications* 10, 1 (Dec. 2019), 2557. https://doi.org/10.1038/s41467-019-10617-y

[82] Dexin Shi, Christine DiStefano, Heather L. McDaniel, and Zhehan Jiang. 2018. Examining Chi-Square Test Statistics Under Conditions of Large Model Size and Ordinal Data. *Structural Equation Modeling: A Multidisciplinary Journal* 25, 6 (Nov. 2018), 924–945. https://doi.org/10.1080/10705511.2018.1449653

[83] Amit Kumar Sikder, Leonardo Babun, Z Berkay Celik, Abbas Acar, Hidayet Aksu, Patrick McDaniel, Engin Kirda, and A Selcuk Uluagac. 2020. Kratos: Multi-user multi-device-aware access control system for the smart home. In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 1–12.

[84] Jason L. Snyder and Mark D. Cistulli. 2011. The relationship between workplace e-mail privacy and psychological contract violation, and their influence on trust in top management and affective commitment. *Communication Research Reports* 28, 2 (2011), 121–129. https://doi.org/10.1080/08824096.2011.565270 Publisher: Routledge tex.owner: siegel tex.timestamp: 2020-01-27.

[85] Anna Squicciarini, Sarah Rajtmajer, Yang Gao, Justin Semonsen, Andrew Belmonte, and Pratik Agarwal. 2022. An extended ultimatum game for multi-party access control in social networks. *ACM Transactions on the Web (TWEB)* 16, 3 (2022), 1–23.

[86] Elena Stephan, Nira Liberman, and Yaacov Trope. 2011. The effects of time perspective and level of construal on social distance. *Journal of experimental social psychology* 47, 2 (2011), 397–402.

[87] Jose M. Such and Natalia Criado. 2016. Resolving Multi-Party Privacy Conflicts in Social Media. *IEEE Transactions on Knowledge and Data Engineering* 28, 7 (2016), 1851–1863. https://doi.org/10.1109/TKDE.2016.2539165

[88] Jose M Such and Natalia Criado. 2018. Multiparty privacy in social media. *Commun. ACM* 61, 8 (2018), 74–81.

[89] Jenny Tang, Eleanor Birrell, and Ada Lerner. 2022. Replication: How well do my results generalize now? The external validity of online privacy and security surveys. In *Eighteenth symposium on usable privacy and security (SOUPS 2022)*. USENIX Association, Boston, MA, 367–385. https://www.usenix.org/conference/soups2022/presentation/tang

[90] Cláudio V Torres, Shalom H Schwartz, and Thiago G Nascimento. 2016. The refined theory of values: associations with behavior and evidences of discriminative and predictive validity. *Psicologia USP* 27 (2016), 341–356. Publisher: SciELO Brasil.

[91] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2014. Intruders versus intrusiveness: teens' and parents' perspectives on home-entryway surveillance. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. 129–139.

[92] Graham Vaughan and Michael A Hogg. 2005. Introduction to social psychology. (2005). Publisher: Pearson Education Australia.

[93] Alvaro Vergés. 2022. On the Desirability of Social Desirability Measures in Substance Use Research. *Journal of Studies on Alcohol and Drugs* 83, 4 (July 2022), 582–587. https://doi.org/10.15288/jsad.2022.83.582

[94] Lin Wang, Xitao Fan, and Victor L. Willson. 1996. Effects of nonnormal data on parameter estimates and fit indices for a model with latent and manifest variables: An empirical study. *Structural Equation Modeling: A Multidisciplinary Journal* 3, 3 (Jan. 1996), 228–247. https://doi.org/10.1080/10705519609540042

[95] Yang Wang, Huichuan Xia, Yaxing Yao, and Yun Huang. 2016. Flying eyes and hidden controllers: A qualitative study of people's privacy perceptions of civilian drones in the US. *Proc. Priv. Enhancing Technol.* 2016, 3 (2016), 172–190.

[96] Stephen G West, Aaron B Taylor, Wei Wu, and others. 2012. Model fit and model selection in structural equation modeling. *Handbook of structural equation modeling* 1 (2012), 209–231. Publisher: New York.

[97] R. M. Williams. 1970. *American Society: A Sociological Interpretation*. New York, NY Knopf.

[98] Jakob Wirth, Christian Maier, Sven Laumer, and Tim Weitzel. 2019. Perceived information sensitivity and interdependent privacy protection: a quantitative

study. *Electronic Markets* 29, 3 (2019), 359–378. Publisher: Springer.

[99] Pamela Wisniewski, AKM Islam, Heather Richter Lipford, and David C Wilson. 2016. Framing and measuring multi-dimensional interpersonal privacy preferences of social networking site users. *Communications of the Association for information systems* 38, 1 (2016), 10.

[100] Pamela Wisniewski, Heather Lipford, and David Wilson. 2012. Fighting for my space: Coping mechanisms for SNS boundary regulation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 609–618.

[101] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy perceptions and designs of bystanders in smart homes. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW (Nov. 2019). https://doi.org/10.1145/3359161 Number of pages: 24 Place: New York, NY, USA Publisher: Association for Computing Machinery tex.articleno: 59 tex.issue_date: November 2019.

[102] Günce Su Yılmaz, Fiona Gasaway, Blase Ur, and Mainack Mondal. 2021. Perceptions of Retrospective Edits, Changes, and Deletion on Social Media. In *Proceedings of the Fifteenth International AAAI Conference on Web and Social Media (ICWSM'21)*.

[103] An Gie Yong and Sean Pearce. 2013. A beginner's guide to factor analysis: Focusing on exploratory factor analysis. *Tutorials in quantitative methods for psychology* 9, 2 (2013), 79–94.

[104] Eric Zeng and Franziska Roesner. 2019. Understanding and Improving Security and Privacy in {Multi-User} Smart Homes: A Design Exploration and {In-Home} User Study. In *28th USENIX Security Symposium (USENIX Security 19)*. 159–176.

[105] Bruno D. Zumbo, Anne M. Gadermann, and Cornelia Zeisser. 2007. Ordinal Versions of Coefficients Alpha and Theta for Likert Rating Scales. *Journal of Modern Applied Statistical Methods* 6, 1 (May 2007), 21–29. https://doi.org/10.22237/jmasm/1177992180

A FINAL SCALE WITH INSTRUCTION

You will see several statements concerning other people's privacy. Privacy means not disclosing information without consent of the involved persons. Please indicate how strongly you disagree or agree with these statements.

There is no right or wrong answer. Please answer as honestly and accurately as possible.

Note. We used a scale ranging from 1 ("Strongly disagree") to 7 ("Strongly agree"). The scale anchors 2 ("Disagree"), 3 ("Somewhat disagree"), 4 ("Neither agree nor disagree"), 5 ("Somewhat agree"), and 6 ("Agree") were labelled as well. The scale is intended to be used by taking the mean value of the individual items.

#	Item
1.	I respect other people's privacy without exception.
2.	I value other people's privacy more than most other people do.
3.	It is important for me to protect other people's privacy even when it is difficult to do so.
4.	Other people's privacy is valuable to me.
5.	When posting a photo with my friends online, it is important to ask for their permission first.
6.	It is important to keep myself from looking at other people's screen notifications.
7.	It is okay to listen to conversations of strangers in public places. (r)
8.	It is important to protect other people's privacy even if I need to invest time and efforts to do it.
9.	It is important to protect other people's privacy even if it ruins the fun for me.
10.	It is okay to screenshot conversations from private chats and show them to others. (r)
11.	It is okay to share other's contact information (such as phone number, email) on request, even when I'm not obliged to. (r)
12.	When sharing pictures of tourist attractions, it is important to ensure that nobody can be clearly identified.
13.	It is important to ask for consent before recording someone speaking.

Table 4: Final scale items. Items marked with "(r)" need to be reversed before calculating the scale mean.