Developing a Psychometric Scale to Measure One's Valuation of Other People's Privacy

Rakibul Hasan
Arizona State University, Arizona, USA

Rudolf Siegel
CISPA, Saarbrücken, Saarland

Rebecca Weil
CISPA, Saarbrücken, Saarland

Katharina Krombholz
CISPA, Saarbrücken, Saarland

Abstract

Researchers invested tremendous efforts in understanding and measuring people's perceptions, concerns, attitudes, and behaviors related to privacy risks from data gathering by online platforms, mobile devices, and other technologies. However, technology users often risk other people's privacy by sharing their data actively (e.g., posting photos taken at public places online) or passively (e.g., granting mobile apps to access stored contacts). Moreover, technologies that continuously sense the environment and record behaviors and activities of *everyone* around them (e.g., smart assistants) are becoming pervasive. Thus, an instrument to quantify how much one *values* other people's privacy is essential to understand technology adoption, attitudes and behaviors related to collecting and sharing data about non-users, inform the design of adaptive privacy enhancing technologies, and developing *personalized* technological or behavioral interventions to raise awareness and mitigate privacy risks. This abstract details a preliminary study towards developing such as scale. We report the methods of generating the initial item pool and findings from a pilot survey. We hope to get feedback from the community to improve the research design during the poster presentation.

1 Introduction

Present technologies do not only risk their primary or direct users' privacy, but also risk the privacy of the users' family, friends, as well as strangers around them. For example, mobile applications and online social platforms may get access to details of their users' contacts and use these data for targeted advertising and surveillance purposes [7, 26]. Online sharing of images and videos, particularly, if they were taken in public places, may reveal the identity, location, and other sensitive information of surrounding people, including strangers to the sharer [9, 12, 14, 30, 34]. Thus, in this increasingly connected world, privacy is interdependent [7]: individual's privacy partly depends on other people's data-disclosing behaviors.

Interdependent privacy issues are pervasive and victimizes people whose data were disclosed by other people, sometimes without their consent or even awareness [4, 14]. Many people have experienced personal, social, and professional consequences after their data was disclosed by others—ranging from social embarrassment (e.g., when a non-flattering image of a person is posted online by another co-owner) to being victims of stalking and cyberbullying (e.g., when a meme that was created using an individual's image goes viral [1]). At a collective level, such data-sharing practices allow building detailed profiles of people, even if those people exercise caution when sharing their information (such as obscuring sensitive information [15, 16]) or completely withdraw themselves from the online space due to privacy concerns [32]. Such knowledge about the public has been exploited for political and business purposes. For example, one of the biggest scandals related to data abuse happened before the 2016 US presidential election: Cambridge Analytica lured Facebook users to give up their friends' data, which were used to manipulate people's voting decisions [10]. More recently, ClearView AI—a company that scraped billions of images from the internet and used them to train a facial recognition application—was heavily criticized by privacy researchers and activists because the company did not obtain consent from the photo uploaders or the people who appeared in those photos [5, 17, 23]. ClearView's service can be used to track any person in the photo database, posing great risks to the privacy, safety, and autonomy of people, including those who never had uploaded their photos on the internet.

Researchers have proposed privacy-enhancing technologies

USENIX Symposium on Usable Privacy and Security (SOUPS) 2022.
August 7–9, 2022, Boston, MA, United States.

(PETs) to mitigate privacy risks of data subjects when their data are shared by other people. For example, Hasan et al. built a machine learning-based tool to automatically detect 'bystanders' in images [14], so that photo owners can protect their privacy by, e.g., obfuscations [15,16], before posting those images online. In the smart home contexts, researchers explored ways to provide data subjects (such as paying guests, visitors, and house workers) the option to control data-gathering sensors such as surveillance cameras and smart assistants (e.g., see [38]). Practical adoption of such PETs, however, heavily depends on the altruistic behaviors of the data collectors, owners, and sharers. Using technologies requires time and effort to learn them; additionally, there may be trade-offs between data subjects' privacy and data owners' utility (e.g., obfuscating certain regions in an image may reduce its visual aesthetics [12]). Consequently, one's adoption of PETs will partly depend on how much they value others' privacy, their awareness of risks (to others) resulting from their data-disclosing behaviors, and how concerned they are regarding those risks.

Several scales exist to measure individuals' concerns, attitudes, and behaviors related to their own privacy [6, 8, 22, 33]. Such scales and associated findings, however, are unlikely to generalize to the interdependent privacy contexts. Thus, past research distinguished between concern for the privacy of others and own privacy concerns [19]. In interdependent privacy context, Koohikamali et al. developed a scale to measure the concern about others' privacy (COP) online data-sharing contexts [19]. Baruh and Cemalcilar showed that concern about others' privacy is one dimension of a multidimensional privacy orientation scale and that people who were concerned about others' privacy were less likely to invade informational privacy [6]. Pu and Grossklags quantified people's monetary valuation of their friends' data in the context of using mobile apps [26]. However, a generic measurement instrument to directly quantify how one values others' privacy is yet to be developed.

Given the increasing integration of technologies in people's personal, social, and professional life that continuously sense their surroundings, quantifying and understanding how technology users value other people's privacy is of great importance. Such understandings will inform research on developing *usable* privacy-enhancing tools and processes that simultaneously minimize data subjects' privacy risks. Moreover, technical measures may be futile in some situations, and self-censoring may be the only way to preserve data subjects' privacy (such as sharing a photo meme depicting someone negatively [4]). Past research on employing behavioral nudges to discourage such data sharing reported paradoxical findings: warning about others' privacy violations *increased*, as opposed to decreasing, people's tendency to post memes online [4, 13]. It remains unclear whether study participants devalued meme subjects' privacy or were unaware of privacy risks from sharing others' photo online; a 'valuation' scale can be used to quantify how different factors affect such data sharing decisionsand develop personalized interventions that have been advocated by many researchers after observing small effects of generic behavioral interventions (see [13] for a review).

In this abstract, we report our preliminary study towards developing a scale to measure how much people value others' privacy. We explain the iterative methodologies we followed to generate the initial scale items, and summarize findings from a pilot study evaluating those items. Results suggest that the scale items were comprehensible to the study participants and contained internal consistency.

2 Background and literature review

2.1 Valuation and related constructs

We distinguish among concerns about, attitudes towards, and valuing others' privacy. Values refer to what is important, good, and worthy [36]. Personal values are desirable and stable goals that influence people's preferences and motivate behaviors across situations [29]. 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) [35]. Attitudes, differently from values, can be context sensitive [28]. Importantly, attitudes could be value expressive [20]; 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 [3]. Concerns can be considered a specific type of an attitude, namely a negative affect toward a certain attitude object [31]. Taken together, assessing others' privacy as a value enables a more accurate 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.

2.2 Related scales in the literature

Several scales exist in the literature to measure one's concerns, attitudes, and behaviors relating to privacy in the context of using technologies, but almost all of them focus on the users' privacy risks [6, 8, 22]. One of the most popular scale was developed by Malhotra et al. that measures measures the degree to which internet users' are concerned regarding data collection, users' control over the data (i.e., raise opinion or opt out), and users' awareness of how the data is used (or how transparent the data usage policy is) [22]. Buchanan et al. extended that scale and proposed three scales to measure privacy related attitudes and behaviors in the context of online data sharing [8]. Baruh and Cemalcılar developed a privacy orientation scale to measure people's information sharing and seeking behaviors on social media [6]. Beyond identifying

factors affecting online information-disclosing behaviors that may impact one's privacy, the researchers also found that concerns about others' privacy impacts how one observes information shared by other people.

Few studies devoted to understanding and measuring privacy concerns and attitudes touched on the interdependent nature of privacy. Wirth et al. examined how concerns' for own and others' privacy and perceived enjoyment from information disclosure (according to Communication Privacy Motivation framework) influence a co-owner's (to whom the original owners shared some information) willingness to protect the original owners' privacy [37]. They developed a theoretical model and empirically validated it supporting the hypothesis that concerns for others' privacy affects data-sharing behaviors. Ozdemir et al. studied how prior privacy experience (e.g., privacy violated by online friends), trust on online friends their awareness of privacy violations contribute to one's privacy concerns [25]. Pu and Grossklags studied how much interdependent privacy contributes to people's decision in adopting social media relative to other factors [26]. In another online study, the authors quantified people's valuations of own and friends privacy in terms of money [27].

Most related to our study, Koohikamali et al. created a scale for concerns about others' privacy (COP) [19].Their study greatly contributes in quantifying COP and it's effects on data-sharing behaviors; unfortunately, the study focused only on the social media, contextualized with certain assumptions (such as victims of privacy violations have no control or power to negotiate with data sharers), and the scale was validated with a university student population [19]. These design choices limits the scale's applicability.

3 Method

The objective of the current study is to develop a scale assessing to which level people value others' privacy. To generate the initial item pool, we followed the guidelines by [18, 24] and used a mixed approach of deductive (i.e., deriving items from a theoretical perspective, e.g. a literature review) and inductive (i.e., creating items by asking people how they perceive a certain topic or behavior [18]) item creation.

Item generation. Items were generated in three different ways. First, we derived items from a literature review; in particular, we borrowed items under "Factor 4: Concern about the privacy of others" from Baruh and Cemalcılar [6]. Second, the authors individually created items related to the target construct. Third, we requested colleagues at our institutions to participate in an online survey that asked them *how they would ask people whether they value other people's privacy or not* (see [21] for a similar approach). Nine people completed this survey; they were experts in cybersecurity and privacy, law (e.g., data privacy officers) and psychology, and administrative people who were not directly involved in research. Thus, we combined several sources to ensure broad and valid coverage of our construct and created 87 items in total.

Refining items. Two of the authors grouped similar items together to identify common themes, reformulated them to be short and precise, and removed duplicates or items that did not fit our measured construct or when their meaning was unclear (e.g., "My privacy has been violated by other people sharing my data"). Then, we sent the revised items to two security experts and 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 refined based on their suggestions. The final list contains 39 items reflecting the following themes: i) valuing others' privacy in general (e.g., "I respect other people's privacy"), ii) present behaviors (e.g., "I always do my best not to intrude into other people's privacy"), iii) opinions on circumstances that affect other people's privacy (e.g., "People using wearable cameras in public places put other people's privacy at risk."), and iv) past experiences (e.g., "People have been angry about me because I have shared their information without consent."). All items are listed below (15 items were reverse coded):

1. I don't care about other people's privacy.(reversed)
2. I respect other people's privacy.
3. I value other people's privacy.
4. It is important for me to protect other people's privacy.
5. It is important for me to protect other people's privacy even when it is difficult to do so.
6. Other people are often too paranoid about their privacy.(reversed)
7. I own information I obtain about others.(reversed)
8. Other people are often too worried about their privacy.(reversed)
9. Other people's privacy is valuable to me.
10. Before posting a photo with my friends online, I ask for their permission.
11. Before sharing a friends phone number on request, I first ask for their permission.
12. Before sharing information, I do my best to prevent violating others' privacy.
13. I do my best not to intrude into other people's privacy.
14. I keep myself from looking at other people's screen notifications.
15. I don't look at other people's phones when they interact with it on the bus.
16. I listen to conversations of strangers in public places.(reversed)
17. I protect other people's privacy even if it has negative consequences for me.
18. I protect other people's privacy even if it ruins the fun for me.
19. I screenshot conversations from private chats and show them to others.(reversed)
20. I share other's contact information (such as phone number, email) on request, even when I'm not obliged to.(reversed)
21. I share photos of people who are unfamiliar to me but might be recognized by others.(reversed)
22. I share private information about other people without their consent.(reversed)

23. When I interact with others, I respect their privacy.
24. When sharing pictures of tourist attractions, I ensure that nobody can be clearly identified.
25. I have been accused of violating someone else's privacy.(reversed)
26. People have been angry with me for sharing their information without consent.(reversed)
27. I have asked people for permission before taking their photograph.
28. I have asked for consent before recording someone speaking.
29. A crime needs to be serious to justify a search warrant for someone's phone.
30. Care should be taken when disclosing information about other people.
31. Everyone has a right to keep their information private.
32. For safety reasons, CCTV is necessary, even when it invades other people's privacy.(reversed)
33. I don't like that some apps on my smartphone require access to my contacts.
34. Most of the time when using technologies, it is unavoidable to violate someone's privacy.(reversed)
35. Other people's need for privacy should be considered when disclosing information about them.
36. People using wearable cameras in public places put other people's privacy at risk.
37. Sharing pictures of babies needs the consent of their parents.
38. When other people give me their phone number, I can use it for any purpose.(reversed)
39. When someone shares their picture, they have lost their right to keep it private.(reversed)

Online survey. We assessed the items' comprehensibility and internal consistency through an online survey (N=50) created on Qualtrics [2] and advertised via Prolific. Participants rated the items using a 7-point Likert scale (*Strongly disagree* to *Strongly agree*). We instructed the participants to not answer an item if they were unclear, or they have other problems answering it, and instead describe their issues in a free text space provided with each item (comparable to the think-aloud technique). We also asked 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.

4 Findings

4.1 Participants

The median completion time for the study was 4.3 minutes, and 75% of the participants completed the survey in 6.2 minutes. Participants were paid $1.2 for their time. Response from one participant was discarded due to quality issues. 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), homemaker (N=4), unemployed (N=4), retired (N=1), and unspecified (N=3).

4.2 Item comprehensibility

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.

4.3 Item consistency and variability

The Cronbach's alpha for the items was 0.91, indicating overall good internal consistency among the items (alpha greater than 0.7 is considered acceptable) [11]. The inter-item correlation was between -0.15 and 0.71. Most correlations were between 0.32 and 0.55. Most items demonstrated wide variability across participants; but, we also identified a few items that were left-skewed or only provoked answers on the middle of the scale. We will list sample items in the poster to initiate discussion with the audience and get experts' feedback and suggestion. We refrained from factor analyses at this stage since our pilot data set was small.

5 Conclusions and future work

To conclude, most of our items were easily comprehensible to the participants. However, some items need rewording to be applicable to all participants. The correlations of our items with each other showed high consistency. Only a few items showed low variability across participants.

In the next step, we will conduct a larger-scale study after revising the existing items as well as adding new items if needed. Data from that study will be used to conduct an exploratory factor analysis to identify latent constructs. Once we achieve a stable and robust factor structure and the final set of scale items well-correlated to those factors, we will administer another study with a new sample to conduct an confirmatory factor analysis and investigate convergent and discriminatory validity of the scale. Presenting the preliminary findings at SOUPS will allow us to get feedback, and simultaneously, we believe that our contribution will benefit researchers working on usable privacy and security.

Acknowledgments

We thank colleagues at CISPA and Arizona State University, and Dr. Shawn Fagan (Indiana University Bloomington) for their participation in the surveys and valuable suggestions in improving this research.

References

[1] 10 Internet memes that ruined lives, 2016.

[2] Qualtrics. https://www.qualtrics.com, 2020.

[3] Icek Ajzen. Values, attitudes, and behavior. In *Methods, theories, and empirical applications in the social sciences*, pages 33–38. Springer, 2012.

[4] Mary Jean Amon, Rakibul Hasan, Kurt Hugenberg, Bennett I Bertenthal, and Apu Kapadia. 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, 5 2020.

[5] Mark Andrejevic and Neil Selwyn. Facial recognition technology and the end of privacy for good., 2020.

[6] Lemi Baruh and Zeynep Cemalcılar. It is more than personal: Development and validation of a multidimensional privacy orientation scale. *Personality and Individual Differences*, 70:165–170, 2014.

[7] Gergely Biczók and Pern Hui Chia. Interdependent privacy: Let me share your data. In *International conference on financial cryptography and data security*, pages 338–353, 2013.

[8] Tom Buchanan, Carina Paine, Adam N. Joinson, and Ulf-Dietrich Reips. 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):157–165, 2007.

[9] Mauro Cherubini, Kavous Salehzadeh Niksirat, Marc-Olivier Boldi, Henri Keopraseuth, Jose M. Such, and Kévin Huguenin. When forcing collaboration is the most sensible choice: Desirability of precautionary and dissuasive mechanisms to manage multiparty privacy conflicts. *Proc. ACM Hum.-Comput. Interact.*, 5(CSCW1), apr 2021.

[10] Wikipedia contributors. Facebook–cambridge analytica data scandal. https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal, 2022. Accessed: 2022-03-29.

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

[12] Rakibul Hasan. Reducing Privacy Risks in the Context of Sharing Photos Online. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems, To appear*, CHI EA '20, New York, NY, USA, 2020. ACM.

[13] Rakibul Hasan, Bennett I Bertenthal, Kurt Hugenberg, and Apu Kapadia. 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, 2021.

[14] Rakibul Hasan, David Crandall, and Mario Fritz Apu Kapadia. Automatically Detecting Bystanders in Photos to Reduce Privacy Risks. In *2020 IEEE Symposium on Security and Privacy (SP)*, Los Alamitos, CA, USA, 5 2020. IEEE Computer Society.

[15] Rakibul Hasan, Eman Hassan, Yifang Li, Kelly Caine, David J Crandall, Roberto Hoyle, and Apu Kapadia. 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, pages 47:1–47:13, New York, NY, USA, 2018. ACM.

[16] Rakibul Hasan, Yifang Li, Eman Hassan, Kelly Caine, David J. Crandall, Roberto Hoyle, and Apu Kapadia. 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*, volume 14, page 25. ACM, 2019.

[17] Kashmir Hill. The Secretive Company That Might End Privacy as We Know It., 2020.

[18] Timothy R. Hinkin. A brief tutorial on the development of measures for use in survey questionnaires. *Organizational Research Methods*, 1(1):104–121, 1998.

[19] Mehrdad Koohikamali, Daniel A Peak, and Victor R Prybutok. Beyond self-disclosure: Disclosure of information about others in social network sites. *Computers in Human Behavior*, 69:29–42, 2017.

[20] Gregory R Maio and James M Olson. What is a "value-expressive" attitude. *Why we evaluate: Functions of attitudes*, 249269, 2000.

[21] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. Internet users' information privacy concerns (iuipc). *Information Systems Research*, 15(4):336–355, 2004.

[22] Naresh K Malhotra, Sung S Kim, and James Agarwal. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, 15(4):336–355, 2004.

[23] By Craig McCarthy and Aaron Feis. Rogue NYPD cops are using facial recognition app Clearview., 2020.

[24] Fabiane F. R. Morgado, Juliana F. F. Meireles, Clara M. Neves, Ana C. S. Amaral, and Maria E. C. Ferreira. Scale development. *Psicologia: Reflexão e Crítica*, 30(1).

[25] Zafer D Ozdemir, H Jeff Smith, and John H Benamati. Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. *European Journal of Information Systems*, 26(6):642–660, 2017.

[26] Yu Pu and Jens Grossklags. 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.

[27] Yu Pu and Jens Grossklags. Towards a Model on the Factors Influencing Social App Users' Valuation of Interdependent Privacy. *Proceedings on Privacy Enhancing Technologies*, 2016(2):61–81, 2016.

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

[29] Lilach Sagiv, Sonia Roccas, Jan Cieciuch, and Shalom H. Schwartz. Personal values in human life. *Nature Human Behaviour*, 1(9):630–639, September 2017. Bandiera_abtest: a Cg_type: Nature Research Journals Number: 9 Primary_atype: Reviews Publisher: Nature Publishing Group Subject_term: Human behaviour;Psychology Subject_term_id: human-behaviour;psychology.

[30] Kavous Salehzadeh Niksirat, Evanne Anthoine-Milhomme, Samuel Randin, Kévin Huguenin, and Mauro Cherubini. "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*, DIS '21, pages 104–124, New York, NY, USA, 2021. Association for Computing Machinery.

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

[32] Manya Sleeper, Rebecca Balebako, Sauvik Das, Amber Lynn McConahy, Jason Wiese, and Lorrie Faith Cranor. The Post That Wasn'T: Exploring Self-censorship on Facebook. In *Proceedings of the 2013 Conference on Computer Supported Cooperative Work*, CSCW '13, pages 793–802, New York, NY, USA, 2013. ACM.

[33] Jason L. Snyder and Mark D. Cistulli. 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):121–129, 2011.

[34] Jose M. Such, Joel Porter, Sören Preibusch, and Adam Joinson. Photo privacy conflicts in social media: A large-scale empirical study. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI '17, page 3821–3832, New York, NY, USA, 2017. Association for Computing Machinery.

[35] Graham Vaughan and Michael A Hogg. Introduction to social psychology. 2005.

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

[37] Jakob Wirth, Christian Maier, Sven Laumer, and Tim Weitzel. Perceived information sensitivity and interdependent privacy protection: a quantitative study. *Electronic Markets*, 29(3):359–378, 2019.

[38] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. Privacy perceptions and designs of bystanders in smart homes. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), nov 2019.