
Reaching Beyond Borders: Investigating Differences in Privacy Harms Concerns

Agnieszka Kitkowska
Karlstad University
Karlstad, Sweden
agnieszka.kitkowska@kau.se

Abstract

Are people worried about harms that may result from their privacy decisions? How can we improve privacy decisions, and make them more informed? In this short position paper, we present some of the findings from the quantitative study on privacy attitudes and behaviors. Further, we shift the attention to potential differences of privacy perceptions among representatives from various demographics. We hope to start the discussion about a necessity to enrich privacy research and include cultural factors, to ensure inclusion and enhance digital privacy.

Author Keywords

Privacy harms; Attitude; Behavior; Culture; Decision-making.

ACM Classification Keywords

H.1.2 [Information Systems]: Models and Principles—*user / machine systems*; K.4.1. [Computers and Society]: Public Policy Issues—*privacy*

Introduction

Over the last decade, digital privacy gained a lot of attention from policymakers, journalists, and scientists, mainly due to the ongoing security and privacy breaches. The experts started to publicly share the best practices for privacy protection. Regardless, people still disclose their sensitive information to online service providers. Is it because the

representation of privacy risks is inadequate to what people are worried about? Can we identify groups of people differing in the level of privacy concerns? What are the factors affecting such groups?

Investigating privacy attitudes

We tried to respond to some of these questions by investigating privacy concerns. We constructed a study aiming to identify dimensions of privacy concerns [5]. Privacy concerns were well researched in the past, and there are various instruments measuring them. For instance, Concern for Information Privacy (CFIP) [7] or Internet Users Information Privacy Concern (IUIPC) [6]. However, to the best of our knowledge, none of the research in this area focused on *privacy harms*. Hence, we underlined the study with a legal framework. We used *privacy harms* framework defined by Daniel Solove [8]. Solove considered harms at the individual level, identifying 16 *privacy harms* (See the margin box). Because his work was based on the real-life examples acquired from court cases, we thought it is plausible that people perceive *privacy harms* in a similar manner. Therefore, we constructed the new scale measuring, as we call it, *privacy harms concerns* (PHC). We used each individual harm from Solove's work and created three items that addressed it. Next, we measured people's level of agreement with each of the statements, on the scale 0-100 (strongly disagree - strongly agree). The statements were focused on harms in a general privacy context, without focusing on the specific technology, data type etc.

Additionally, we wanted to examine potential demographic differences in the PHC, information disclosure and protection behavior. Hence, we tried to gather participants from different geographic areas, such as the USA, UK, Nordic Countries and Italy. Further, the study included participants from various age (ranging 18-75 years old) and education

Privacy Harms identified by Daniel Solove [8]

Data Collection:

- *surveillance*
- *interrogation*

Data Processing:

- *secondary use*
- *aggregation*
- *exclusion*
- *insecurity*
- *identification*

Data Dissemination:

- *breach of confidentiality*
- *appropriation*
- *disclosure*
- *distortion*
- *blackmail*
- *exposure*
- *increased accessibility*

Invasions:

- *decisional interference*
- *intrusion*

Table 1: Dimensions of privacy harms concerns (Means, Standard Deviation, Reliability for items loaded in each dimension - Cronbach α), $N=382$.

| Dimension | M | SD | α |
|-----------------------|-------|------|----------|
| Insecurity | 90.02 | 10.4 | .736 |
| Exposure | 77.82 | 17.7 | .745 |
| Unauthorized access | 72.75 | 17.2 | .865 |
| Secondary use of data | 72.42 | 20.0 | .811 |
| Misuse of data | 71.23 | 16.1 | .836 |
| Distortion | 63.75 | 21.5 | .736 |
| Interrogation | 45.89 | 21.2 | .721 |

groups. All participants were gathered online, 42 through CallForParticipants, 340 through Microworkers.

Dimensionality of privacy concerns

According to our results, people do not perceive privacy harms at the individual level. Rather, they simplify and generalize harms, presumably making them easier to understand. Regardless, we have found some patterns and similarities within the collected responses. After applying Exploratory Factor Analysis, 30 out of 48 items of the measuring scale remained. Within this set, we identified seven dimensions of privacy harms concerns: *unauthorized access*, *insecurity*, *misuse of data*, *secondary use of data*, *exposure*, *distortion* and *interrogation*. The items that loaded to each of the dimensions had communalities $> .3$, item loadings $> .4$. There were minimum three items loaded on each factor. We checked the internal consistency, and the Cronbach α were all $> .7$ (Table 1). The details on instrument creation are presented in [5].

To further investigate the dimensions of PHC, we validated them against the measurements of information disclosure

Table 2: Participants demographics

| Demographic | N | % |
|------------------|------------|------|
| <i>Country</i> | | |
| Italy | 91 | 23.8 |
| Nordic | 76 | 19.9 |
| UK | 113 | 29.6 |
| USA | 102 | 26.7 |
| <i>Gender</i> | | |
| Male | 221 | 57.9 |
| Female | 161 | 42.1 |
| <i>Education</i> | | |
| High school | 70 | 18.3 |
| Higher education | 203 | 53.1 |
| Still studying | 109 | 28.5 |
| <i>Age</i> | | |
| 18-24 | 98 | 25.7 |
| 25-34 | 153 | 40.1 |
| 35-44 | 76 | 19.9 |
| over 44 | 55 | 14.4 |
| Total | 382 | |

(scale acquired from Joinson et al. [4]) and protection behavior (instrument acquired from Buchanan et al.[1]).

Information disclosure and protection behavior

The study results demonstrated significant differences in perception of privacy harms among respondents who have high (HD) and low (LD) levels of information disclosure. It seems that HD participants were more concerned about the *secondary use of data* and *interrogation* (services probing people to provide personal information, participate in online surveys etc.).

Similarly, Pearson correlation analysis confirmed correlations between the seven dimensions of PHC and protection behaviors. For instance, the participants who apply both technical and general protection methods expressed high levels of concerns about *unauthorized access*, *misuse*, *secondary use of data*, *insecurity*, *exposure* and *distortion*.

Privacy harms as a factor affecting behavior

Although, in research there is an ongoing debate whether attitude predicts behavior, and in the field of privacy a dispute about the *privacy paradox* (people express concerns about their privacy but regardless of such attitude, they disclose personal information), our results suggest that there is a possible influence of PHC on certain types of behavior (disclosure or protection behavior). However, additional studies are required to measure the PHC impact on the actual behavior. Hence, in the future, we plan to confirm findings in experiments examining the causal relationship between concerns and behavior.

Current results are based on an online survey, which measured the information disclosure and protection behavior via an online questionnaire. Even though both instruments were validated in the past research, we realize that the actual effect of harms on privacy behavior should be mea-

sured in experimental settings or with the use of real data sets.

Demographic variety

By inclusion of broad demographics, we aimed to see, whether there are patterns differentiating privacy concerns among individuals (Table 2). According to the results of the One-Way ANOVA, Italian respondents significantly differed from the UK, USA and Nordic respondents in PHC. The respondents from Italy had significantly lower concerns about the *secondary use of data*, *interrogation* and *distortion*. Similarly, respondents from Nordic countries expressed fewer concerns over *distortion* than the USA respondents. Additionally, our results showed that there are significant differences between participants with various education levels. For instance, the respondents with lower education were less concerned about some of the privacy harms than participants who are currently studying. Lastly, the study confirmed that the levels of PHC significantly differ among the respondents from different age groups. In sum, there was a pattern showing that the older generations tend to worry more about their privacy than the younger generations. However, younger generations are more likely to apply privacy protection measures.

Privacy harms and cultural diversity

The main goal of our research was to develop the new scale measuring privacy concerns and investigate how people perceive privacy harms. Regardless, some of the results demonstrate potential cultural/ethnic foundations that shape privacy perceptions. Unlike in the research on the technology acceptance, digital privacy is rarely examined from the cultural perspective. Considering the culture's definitions, such as culture is *the collective programming of the mind which distinguishes the members of one group or category of people from another* [3] and a pat-

tern of thinking, feeling and acting (behavior) that is learned throughout a person's life, beginning in early childhood [2], it becomes clear, that culture plays a prominent role in decision-making. Consequently, it may have an influence on a human-computer interaction and digital privacy.

Hence, we postulate for implementation of culture to the privacy research, to improve understanding of factors underlying privacy attitudes and behaviors. The existing cultural frameworks, such as Hofstede's taxonomy identifying five characteristics of cultural groups: *power distance, individualism, masculinity, uncertainty avoidance, and long-term orientation* [3] could be added to the privacy research. Additionally, the cultural dimensions may be applied not only to investigate differences at the national level but also to examine smaller populations, for instance at the organizational level, or to identify new groups sharing similar privacy attitudes and behaviors. Here, the framework suggested by [9] could be used to investigate cultural differences. Although, defined for social media services, their framework demonstrates how culture, shaped by societal and legal norms, and by user expectations may be used to improve privacy research.

Conclusion

In this short paper, we presented the results of the study about privacy harms concerns. The message we tried to communicate can be summarized two-fold.

First, people tend to perceive privacy harms in a generic and simplified form. Perhaps because it is easier to comprehend and avoid privacy complexity. Even for experts, it may be difficult to identify harms that may result from information disclosure. It appears that there are differences in perception of privacy harms among people with contrasting levels of information disclosure and types of protection be-

havior. Such finding could be useful for privacy designers, for instance to design privacy indicators representing the most severe privacy harms. In the long run, privacy harms could be used as a basis for a design of visual cues, displayed to people at different times of interaction, aiming to enhance informed privacy decisions.

Second, there is a potential that privacy harms are perceived differently by people with various cultural/ethnic backgrounds. There seems to be a lack of privacy research reaching beyond western societies and focusing on cultural differences. The majority of studies is based on the same demographics, mostly students or postgraduates, from USA or Europe, resembling in age etc. While even within the western societies, there may be potential cultural dependencies of privacy concerns. It is obvious that culture-based studies require much more effort, such as larger samples, multilingual instruments, an extensive amount of time etc. Additionally, culture is not a static concept, it evolves together with societal changes, making it a challenge to investigate. However, the entire omission of culture as one of the drivers for privacy-related attitudes and behaviors may result in misleading or false conclusions. It can lead to poorly designed privacy, social exclusion, increasing the divide between members of various demographics. Further, the exclusion of cultural factors diminishes chances to protect individuals and instead promotes privacy designed only for *some*. Similarly to the globally available technology, privacy should become available and accessible beyond borders. This is important especially now when international companies will have to comply with the legal requirements for data protection, such as the General Data Protection Regulation. Therefore, a broader understanding of individuals' privacy decisions could help service providers with the legal compliance and enhance users' privacy.

Acknowledgment

This work has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675730.

REFERENCES

1. 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 Association for Information Science and Technology* 58, 2 (2007), 157–165.
2. Kenneth J Calhoun, James TC Teng, and Myun Joong Cheon. 2002. Impact of national culture on information technology usage behaviour: an exploratory study of decision making in Korea and the USA. *Behaviour & Information Technology* 21, 4 (2002), 293–302.
3. Geert Hofstede. 2011. Dimensionalizing Cultures: The Hofstede Model in Context. *Online Readings in Psychology and Culture* 2, 1 (2011), 1–26.
4. Adam N Joinson, Carina Paine, Tom Buchanan, and Ulf-Dietrich Reips. 2008. Measuring self-disclosure online: Blurring and non-response to sensitive items in web-based surveys. *Computers in Human Behavior* 24, 5 (2008), 2158–2171.
5. Agnieszka Kitkowska, Erik Wastlund, Joachim Meyer, and Leonardo A Martucci. 2017. Is it harmful? Re-examining Privacy Concerns. (2017). (in press).
6. 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.
7. H Jeff Smith, Sandra J Milberg, and Sandra J Burke. 1996. Information privacy: measuring individuals' concerns about organizational practices. *MIS quarterly* 20 (1996), 167–196.
8. Daniel J Solove. 2005. A taxonomy of privacy. *U. Pa. L. Rev.* 154 (2005), 477.
9. Blase Ur and Yang Wang. 2013. A cross-cultural framework for protecting user privacy in online social media. In *Proceedings of the 22nd International Conference on World Wide Web*. ACM, 755–762.