# Is It Harmful? Measuring People's Perceptions of Online Privacy Issues

**Agnieszka Kitkowska**
Karlstad University
Karlstad, 65188, Sweden
agnieszka.kitkowska@kau.se

**Joachim Meyer**
Tel Aviv University
Tel Aviv, 6997801, Israel
jmeyer@tau.ac.il

**Erik Wastlund**
Karlstad University
Karlstad, 65188, Sweden
erik.wastlund@kau.se

**Leonardo A. Martucci**
Karlstad University
Karlstad, 65188, Sweden
leonardo.martucci@kau.se

## Abstract

We report preliminary findings from an online study, identifying people's attitudes toward privacy issues. The results confirm some of the previous research findings regarding demographic and contextual dependencies of privacy perceptions. The research presents a new scale for measuring attitudes to privacy issues that is based on privacy harms. The results suggest that people consider privacy harms in generic and simplified terms, rather than as separated issues suggested in legal research. This research identified major factors that people tend to think of while considering online privacy.

## Author Keywords

Privacy; Human factors; Attitudes; 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

The rapid growth of internet connectivity and the availability of connected devices raise concerns among policy makers and end-users. Modern technologies, equipped with various sensors, enable extensive data collection. New legislation, such as the General Data Protection Regulation

**Privacy Harms identified by Daniel Solove [6]**

**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*

(GDPR), attempt to regulate personal data processing by listing the privacy principles, providing guidelines for online service providers and by enhancing the end-users' fundamental rights [3]. Although GDPR applies only to the EU, it has implications for the foreign companies processing personal data of European citizens. Despite the GDPR and other privacy regulations, the end-users' privacy decisions are frequently poor and uninformed. This may be due to the lack of alignment between the legislation and people's perceptions of privacy issues.

Due to its multidimensional nature, privacy may be perceived in different ways. For example, the term may be used interchangeably with security, anonymity, confidentiality, secrecy or ethics [8]. Due to this diversity, it is possible that privacy issues in legal context, may differ from end-users perceptions of privacy. Daniel Solove identified 16 privacy harms based on legal cases (see sidebar) and created a framework for future law and policy makers [6]. Considering privacy as a social concept, and focusing on issues invading personal privacy, Solove aimed to show the uniqueness of each privacy harm, related to individual activities. The framework assigned harms to four groups, defined according to the data processing actions, considering both end-users and data processors.

## Research goals

The goal of this research is to compare privacy harms identified by Solove with people's perceptions of importance and severity of privacy issues. Also, we intend to measure possible effects of demographic variables on perceptions of privacy risks and issues. To achieve these goals we created the new measuring scale based on the privacy harms identified by Daniel Solove [6]. Solove's harms were fundamental because they originate from court cases. Therefore, we assume that such privacy harms, extracted from real-life scenarios, should be present in people's mental representations of privacy issues, at least to some degree.

## Method

We created an online survey containing scales measuring privacy attitudes and behaviors. We created the 48 items scale derived from the Solove's 16 privacy harms (three items related to each of the privacy harms). The other scales were adopted from previous research to measure online information disclosure [2] and protection behaviors [4].

*Participants*

The online survey was distributed on Microworkers and CallForParticipants (CFP). Microworkers' participants received \$1-\$1.50 per response. The CFP participation was voluntary. The total number of participants reached 437 but 382 responses were valid. Among the respondents 57.9% ($N = 221$) were males and 42.1% ($N = 161$) females; the average age was 32 years ($Min = 18, Max = 70$). Choice of geographic areas was based on the data from the Data Protection Eurobarometer [7]. The geographic location covered four areas: UK, USA, Italy and Nordic countries (Sweden, Norway, Finland, Denmark and Germany); 18.3% ($N = 70$) of participants had no higher education, 53.1% ($N = 203$) had higher education, and 28.5% ($N = 109$) were still studying.

## Results

We first computed the means of the items in the scale. We grouped them accordingly to Solove's framework to evaluate whether some of the privacy issues are perceived as more severe than others (Table 1).

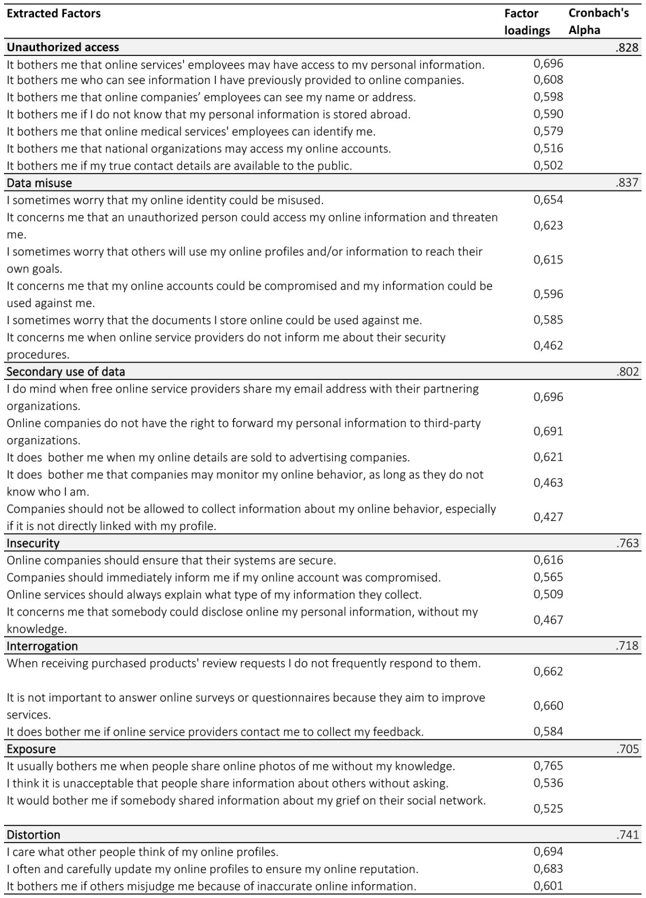
Regarding the *data collection*, we found concerns about employer's social media surveillance (*surveillance* $I$) and

| ***Item*** | ***M*** | ***SD*** |
|---|---|---|
| ***Collection*** | | |
| Surveillance $I$ | 70.03 | 28.1 |
| Surveillance $II$ | 72.76 | 21.9 |
| ***Processing*** | | |
| Insecurity | 94.15 | 9.8 |
| Exclusion | 88.32 | 14.7 |
| Secondary Use | 82.16 | 23.2 |
| ***Dissemination*** | | |
| Data Breach | 93.58 | 11.0 |
| Accessibility $I$ | 82.50 | 21.7 |
| Accessibility $II$ | 82.03 | 22.8 |
| Disclosure $I$ | 84.04 | 18.5 |
| Disclosure $II$ | 83.59 | 17.3 |
| Exposure | 83.28 | 18.5 |
| ***Intrusions*** | | |
| Intrusion $I$ | 73.31 | 21.8 |
| Intrusion $II$ | 51.27 | 25.3 |
| Decisional Interference | 47.4 | 26.3 |

**Table 1:** Means for individual items of the new measuring scale, *N*=382.

national organizations accessing online accounts (*surveillance* $II$). Considering *data processing*, respondents agree that companies should ensure security (*insecurity*) and provide information about data collection (*exclusion*), and they should not forward personal information to third parties (*secondary use*). Regarding *data dissemination*, respondents agree that companies should immediately inform users about security breaches (*data breach*), guarantee access to deletion or amendment of personal information (*accessibility* $I$ and *accessibility* $II$). We found concerns about the type of data visible to others (*disclosure* $I$) and data disclosed without permission (*disclosure* $II$, *exposure* - information about grieving). Considering *invasions*, respondents were less unidirectional. The results showed that respondents are annoyed by online advertisements (*intrusion* $I$), but less concerned about buying suggestions (*decisional interference*) or advertising messages (*intrusion* $II$).

We conducted an Exploratory Factor Analysis (EFA) to analyze the new scale. The Kaiser-Meyer-Olkin measure was $.903$ and Bartlett sphericity test was significant ($p < .001$) which suggests EFA's suitability. To extract factors we used the principal axis factoring (PAF) allowing measuring latent structure of the variables and their relationships [5]. From the original 48 items 31 items remained, after removing factors with communalities $< .3$, factor loadings $< .3$ and factors consisting of less than three loaded items. After the scale reduction and scree plot analysis, we extracted seven factors, identifying people's perceptions of privacy issues: *unauthorized access, data misuse, secondary use of data, insecurity, data exposure, interrogation, distortion*. When computing the internal consistency for scales based on the factors, the Cronbach alpha scores for the factors were all above $.7$ (Fig. 1).



| **Extracted Factors** | **Factor loadings** | **Cronbach's Alpha** |
|---|---|---|
| **Unauthorized access** | | .828 |
| It bothers me that online services' employees may have access to my personal information. | 0,696 | |
| It bothers me who can see information I have previously provided to online companies. | 0,608 | |
| It bothers me that online companies' employees can see my name or address. | 0,598 | |
| It bothers me if I do not know that my personal information is stored abroad. | 0,590 | |
| It bothers me that online medical services' employees can identify me. | 0,579 | |
| It bothers me that national organizations may access my online accounts. | 0,516 | |
| It bothers me if my true contact details are available to the public. | 0,502 | |
| **Data misuse** | | .837 |
| I sometimes worry that my online identity could be misused. | 0,654 | |
| It concerns me that an unauthorized person could access my online information and threaten me. | 0,623 | |
| I sometimes worry that others will use my online profiles and/or information to reach their own goals. | 0,615 | |
| It concerns me that my online accounts could be compromised and my information could be used against me. | 0,596 | |
| I sometimes worry that the documents I store online could be used against me. | 0,585 | |
| It concerns me when online service providers do not inform me about their security procedures. | 0,462 | |
| **Secondary use of data** | | .802 |
| I do mind when free online service providers share my email address with their partnering organizations. | 0,696 | |
| Online companies do not have the right to forward my personal information to third-party organizations. | 0,691 | |
| It does  bother me when my online details are sold to advertising companies. | 0,621 | |
| It does  bother me that companies may monitor my online behavior, as long as they do not know who I am. | 0,463 | |
| Companies should not be allowed to collect information about my online behavior, especially if it is not directly linked with my profile. | 0,427 | |
| **Insecurity** | | .763 |
| Online companies should ensure that their systems are secure. | 0,616 | |
| Companies should immediately inform me if my online account was compromised. | 0,565 | |
| Online services should always explain what type of my information they collect. | 0,509 | |
| It concerns me that somebody could disclose online my personal information, without my knowledge. | 0,467 | |
| **Interrogation** | | .718 |
| When receiving purchased products' review requests I do not frequently respond to them. | 0,662 | |
| It is not important to answer online surveys or questionnaires because they aim to improve services. | 0,660 | |
| It does bother me if online service providers contact me to collect my feedback. | 0,584 | |
| **Exposure** | | .705 |
| It usually bothers me when people share online photos of me without my knowledge. | 0,765 | |
| I think it is unacceptable that people share information about others without asking. | 0,536 | |
| It would bother me if somebody shared information about my grief on their social network. | 0,525 | |
| **Distortion** | | .741 |
| I care what other people think of my online profiles. | 0,694 | |
| I often and carefully update my online profiles to ensure my online reputation. | 0,683 | |
| It bothers me if others misjudge me because of inaccurate online information. | 0,601 | |

**Figure 1:** EFA results. Factor loadings and Cronbach's alpha reliability.

*Demographic differences*

We computed scores for the seven scales based on the factors, and conducted One-Way Analysis of Variance (ANOVA), comparing with means for the scales between different geographic locations. There were significant effects for *secondary use of data* ($F(3, 381) = 5.010, p = .002$), *interrogation* ($F(3, 381) = 3.241, p = .022$) and *distortion* ($F(3, 381) = 2.885, p = .036$).

The post-hoc Tukey test resulted in significant difference ($p = .001$) between Italy ($M = 77.2, SD = 19.9$) and the UK ($M = 77.2, SD = 17.9$) regarding the *secondary use*. Similarly, there was significant difference ($p = .038$) between Italy ($M = 40.3, SD = 20.5$) and the Nordic Countries ($M = 49.8, SD = 19.7$), and Italy and the UK ($M = 48.3, SD = 20.7$), ($p = .034$) related to *interrogation*. We found significant difference ($p = .017$) between the USA ($M = 68.4, SD = 20.1$) and Nordic Countries ($M = 60.6, SD = 19.7$), and the USA and Italy ($M = 60.4, SD = 23.0$) about *distortion* ($p = .010$).

Additionally, perceptions of *data misuse* differed between education groups ($F(2, 381) = 4.543, p = .011$). There was a significant difference between high school (HS) ($M = 67.7, SD = 15.7$) and still studying (SS) ($M = 74.7, SD = 16.5$)($p = .012$) respondents. Similarly, groups' perceptions of *insecurity* differ ($F(2, 381) = 3.621, p = .028$) among HS ($M = 88.2, SD = 19.8$) and SS ($M = 92.4, SD = 9.4$); *distortion* ($F(2, 381) = 4.401, p = .013$) between HS ($M = 60.2, SD = 20.9$) and SS ($M = 69.9, SD = 17.5$).

## Discussion

We created a new scale to measure people's attitudes to privacy issues and whether their opinions differ demographically. Additionally, we wanted to see whether the Solove's framework of privacy harms corresponds with people's perceptions.

Firstly, the preliminary analysis of means show that people differentiate in perceptions of privacy harms. The EFA indicates that groupings of privacy harms corresponds only partially with groupings suggested by Solove. This suggests that people's mental representations don't separate harms. People combine harms to comprehensive, generic mental representations, such as *insecurity* or *unauthorized access* in general. However, the results suggest that people recognize *data exposure*, *distortions* and *interrogation* as categories of harms corresponding with the three privacy harms defined by Solove.

Our results also show possible differences in the perceptions of privacy issues between people from different countries and with different educational level. This may be due to the role of the *context* such as social norms or culture [1]. This suggests that people may have different expectations regarding privacy protection, depending on various demographics. Therefore, developers and designers who, according to the new GDPR, should ensure an appropriate level of privacy communication [3], must find new ways to indicate privacy issues, avoiding misconceptions of privacy.

## Future work

The study is a first step in an extended research program on privacy perceptions. The next step is to focus on the perceived severity of the privacy harms and to identify whether there is a relationship between the new attitudes scale and information disclosure, and protection behavior. That could contribute understanding of privacy related attitudes and behaviors.

## REFERENCES

1. L. Barkhuus. The Mismeasurement of Privacy: Using Contextual Integrity to Reconsider Privacy in HCI. In *ACM SIGCHI Conference on Human Factors in Computing Systems*, pages 367–376, 2012.

2. T. Buchanan, C. Paine, A. N. Joinson, and U.-D. 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.

3. EU. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. *Official Journal of the European Union*, (April), 2016.

4. A. N. Joinson, C. Paine, T. Buchanan, and U. D. Reips. Measuring self-disclosure online: Blurring and non-response to sensitive items in web-based surveys. *Computers in Human Behavior*, 24(5):2158–2171, 2008.

5. T. G. Reio and B. Shuck. Exploratory factor analysis: Implications for theory, research, and practice. *Advances in Developing Human Resources*, 17(1):12–25, 2015.

6. D. Solove. A taxonomy of privacy. *University of Pennsylvania Law Review*, (477):477–560, 2006.

7. TNS Opinion & Social. Europeans' attitudes towards security. Special Eurobarometer 432. Technical report, 2015.

8. H. Xu, X. R. Luo, J. M. Carroll, and M. B. Rosson. The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision support systems*, 51(1):42–52, 2011.