# Crowdsourcing Privacy Design Critique: An Empirical Evaluation of Framing Effects

Oshrat Ayalon
Tel Aviv University
oshratra@post.tau.ac.il

Eran Toch
Tel Aviv University
erant@post.tau.ac.il

## Abstract

*When designed incorrectly, information systems can thwart people's expectations of privacy. An emerging technique for evaluating systems during the development stage is the crowdsourcing design critique, in which design evaluations are sourced using crowdsourcing platforms. However, we know that information framing has a serious effect on decision-making and can steer design critiques in one way or another. We investigate how the framing of design cases can influence the outcomes of privacy design critiques. Specifically, we test whether 'Personas', a central User-Centered Design tool for describing users, can inspire empathy in users while criticizing privacy designs. In an experiment on Amazon Mechanical Turk workers (n=456), we show that describing design cases by using personas causes intrusive designs to be criticized more harshly. We discuss how our results can be used to enhance privacy-by-design processes and encourage user-centered privacy engineering.*

## 1. Introduction

Over-stepping users' expectations of privacy can be costly. Surprising users by sharing their data with unexpected people and organizations or using data in unexpected ways can deter users from using a system [21, 36] or push them to choose other alternatives [19, 47]. Privacy-by-design (PbD) initiatives propose a design and development framework that aids in the production of privacy-respectful systems [10, 34]. These initiatives can involve, for example, organizational processes such as Privacy Impact Assessment (PIA) [58] and patterns for designing ubiquitous systems that minimize the amount of collected data [34]. The U.S. FTC's acknowledgement of PbD [61] as a mandatory part of the EU General Data Protection Regulation (EUGDPR) [20], which is planned to take effect at 2018, has drawn considerable attention to PbD and to the challenges in implementing it. Critics have pointed to serious flaws in PbD, such as its lack of necessary technical focus [50], its disconnect from existing business practices [54], its rigidity [32], and its stark differences from engineering mindsets [7]. The challenge of implementing PbD requires further thinking on how system design decisions can be made in contexts that encourage privacy.

Privacy cannot be viewed solely as a legal issue, and privacy aspects of system design can impact the experiences of users to a considerable degree. Previous studies have shown that developers and other people making decisions on information system privacy design consult with engineers [5, 28] or Chief Privacy Offices (CPOs) [5, 6]. However, without consulting end-users directly, designers fail to determine users' perceptions of privacy expectations. An illustrative case study is the enrollment of Google Buzz, a social network launched in 2010. Shortly after its launch, several serious privacy flaws were identified, including making Gmail users' contacts public by default [54]. In response to public uproar, Google rescinded the feature a week after launch and discontinued the service approximately one year later. Even though the feature was initially used by Google employees, danah boyd argues that internal testing is not sufficient because "technologists assume the most optimal solution is the best one, but this tends to ignore a whole bunch of social rituals that have value." [9] While some PbD processes involve interaction with users [31], this requirement is very generalized and does not point to a concrete way through which meaningful feedback from users can be efficiently received.

User-centered design (UCD) describes a design approach through which end-users are involved throughout the design process. Focused on usability, UCD requires user feedback, as designers alone cannot reveal all types of usability problems [1]. In this work, we recommend extending UCD to privacy design: collecting feedback on system designs and evaluating the potential for privacy intrusiveness.

Several studies have investigated the use of feedback from non-expert crowds on design work [11, 18, 37, 51, 59]. Inspired by these studies, we suggest a methodology for using crowdsourcing to evaluate privacy design decisions. When considering how to

URI: http://hdl.handle.net/10125/50487
ISBN: 978-0-9981331-1-9

crowdsource privacy critique, we must account for the effects of information framing on crowds' responses. To be useful, feedback from a crowd should reflect the responses of potential users. One important aspect of this requirement is the framing of privacy design questions. Our search for making privacy design decisions had led us to consider empathy theory. The empathy cognitive approach focuses on the recognition and understanding of someone else's thoughts and feelings by "*walking in another's shoes*" [16]. In UCD, *Personas*, which are "hypothetical archetypes of actual users" [13], are used to communicate information on end-users between designers and engineers. In UCD, personas are arguably a way to encourage empathy toward end-users by putting a human face on the generic user [38, 40, 41, 49]. However, the capacities for personas to encourage empathy are questionable, and it is unclear whether empathy extends to privacy decisions.

We present a study that investigates how the presentation of design scenarios whether explained through data descriptions or the use of basic or detailed personas affects design decisions. Following a methodology used in behavioral economics to assess effects of the presentation of information on decisions based on large crowds [3, 53], we conducted an online experiment that involved administering a questionnaire to 456 non-expert participants recruited via Amazon Mechanical Turk (AMT), a crowdsourcing service. We found that framing design questions using personas results in fewer privacy intrusive design decisions. By delivering the first experimental and large-scale evaluation of the effects of personas on privacy design decisions, we aim to encourage a discussion on the roles of UCD and design decisions in the context of privacy.

## 2. Background

### 2.1. Privacy-by-Design

Privacy-by-Design applies principles and processes to analyze and improve the privacy of information systems and procedures. It advocates for mitigating privacy threats from the very start rather than by adding layers of privacy-enhancing technologies after the fact when it can be too late to solve inherent privacy problems [10, 34]. PbD was criticized for being too technical and not considering the complex contexts involved in developing real-world information systems [32]. Others criticize PbD for its lack of concrete implementation requirements that engineers can follow [27].

The concept of PbD has been mostly studied from a legal perspective. A few studies have investigated developers' approaches to and capabilities in making privacy design decisions. Several studies have shown that developers mostly focus on security and protection against hackers as the most important aspect of privacy rather than on the usage of data by system operators [4, 28]. When required to solve privacy issues, developers may not consider such issues as their responsibility [28] or seek advice within their social networks or organizations [5]. With respect to PbD, Koops et al. [27] state that "fostering the right mindset of those responsible for developing and running data processing systems may prove to be more productive than trying to achieve rule compliance by techno-regulation."

Some PbD white-papers recommend interacting with users through focus groups or by other means [31]. However, this requirement is not viewed as mandatory or essential to PbD. In contrast, we argue that part of a developer's changing mindset can be applied by incorporating end-users' points of view into the design process.

### 2.2. Design Feedback and Crowdsourcing

As we consider turning to end-users for their perceptions and opinions, we turn to former studies on feedback gathering. Feedback is an essential facet of any design process, but finding the right people to provide relevant feedback is not always easy. Several studies have suggested solutions that use non-expert crowds to provide different aspects of feedback. Xu et al. [59] presented Voyant, a system that provides designers with perception-oriented feedback. Robb et al.'s [51] method focused providing interior designers with visual feedback (photos) rather than textual feedback. Dow et al. [18] explored crowd feedback contributions given at different phases of an innovation process, and Chai et al. explored Twitter as a basis for collecting feedback from potential patients on medical procedures [11]. Extending design critiques to privacy may be a practical and cost-effective way to achieve this goal, but the feasibility of this new approach should be tested.

### 2.3. Empathy and Information Presentation

We are considering crowdsourcing as a way to critique privacy design; we ask how crowd workers can consider the end-user's point of view by engaging with the system. In behavioral economics, the works of Tversky and Kahneman [57] provide a theoretical and empirical basis for the effects of information framing on decision-making. Since then, a wide body of literature has shown that emotional stimuli affect decisions, shifting them to more empathic outcomes. These effects were shown to influence the decisions in diverse domains such as charity donations, economics and nature conservation. For example, Chang and Lee [12] showed that images of children increase the probability of people contributing to related charities. Rubinstein [53] found that students tend to make decisions that tend to maximize profits when decisions are framed using mathematical equations. Rode et al. [52] proved that economic discourse framing leads to significantly fewer pro-conservation decisions, even if a cost-benefit analysis shows that the anti-conversation decision is not viable.

### 2.4. Personas

Personas are models for end-users that represent "hypothetical archetypes" who share common objectives, attitudes, needs, wants and behaviors [13]. The definitions of Pruitt & Adlin [49] represent the most accepted form of personas, as "fictitious, specific, concrete representations of target users." Multiple studies have suggested that personas use can increase a product's usability and other end-users' related aspects, such as desirability, enjoyment [29], and the extent to which products "get intimately linked with peoples' lives" [14]. Several scholars and practitioners have argued that personas can allow designers to empathize with the views of different groups of users and to design products that address users' wants and abilities in a better way [14, 29, 39].

Personas have been used extensively in HCI to understand users and to communicate information about users to a broad range of stakeholders in the development process [8, 23, 25, 35, 49]. In the field of usable privacy, Spears and Erete [55] proposed a framework for privacy personas that captures and communicates information about the privacy attitudes, goals and behaviors of users.

One of the main arguments for personas is that personas encourage empathy towards end-users. As Pruitt & Adlin state, "A major virtue of personas is the establishment of empathy and understanding of the individuals who use the product... by empathy, I mean an understanding of and identification with the user population" [8, 49]. Other practitioners and scholars have described personas in a similar way [40, 41]. An ethnographic study [42] supports this notion of personas based on Danish practitioners' reported benefits of using personas. For example, they described how personas have helped them design while considering users' needs:

*"We are still quite technically oriented and nerdy when we develop. Now we describe the customers' needs first [...].This is completely different from what we did before. And personas have helped us understand what needs you are to cover."*

However, other studies have shown only anecdotal support for the notion that personas boost designer empathy towards users [23]. These conflicting results challenge the use of personas for empathetic design in general and of privacy-by-design in particular. Furthermore, even if personas affect empathy, it is unclear whether these results extend to issues of privacy.

### 2.5. Research Questions

In this study we aim to understand whether and how the framing of design questions with personas affects privacy design decisions. Although personas are usually used within a designer's community and not with respect to the general population, our intention remains the same. We want the audience, here non-experts, to develop a better understanding of end-users through the presented privacy problem. We expect that different levels of persona presentation will result in varying levels of empathy toward end-users, eventually affecting the decisions made. In the following section, we further describe how we have defined different levels of personas. Additionally, as we refer to privacy design decision-making by people, we consider a personal aspect: individuals' perceived levels of privacy. We expect decisions related to privacy to be associated with personal perceptions of having privacy. We assume the applications that we test to be general in the sense that any smartphone user can operate them to regard a general crowd as a candidate for the analysis. Our expectations lead us to make the following hypotheses:

**H1.** Design decisions made about privacy are less privacy-intrusive when the level of persona presentation is higher.

**H2.** Design decisions made about privacy are more privacy-intrusive when the perceived privacy, i.e., the extent to which one feels he or she has privacy, is higher.

## 3. Method

### 3.1. Experimental design

To examine our hypotheses, we designed a between-subject user study (n = 456), using an online experiment that included a questionnaire. The main section of the questionnaire was designed to elicit our dependent variable of privacy intrusiveness and measure the effects of different persona presentation levels. The questionnaire also included two other sections: 1) personal aspects including perceived privacy and empathy and 2) demographics. Except for the demographics section, the questions presented statements, and the participants were asked about the extent to which they agreed with each statement. We used a seven-point Likert scale, where 1 represented low agreement and 7 represented high agreement. The study was authorized by the institutional ethics review board (IRB) and occurred in January 2017.

The primary goal of the experiment was to compare effects of the framing of design decisions on the intrusiveness of the chosen design. Accordingly, the participants were randomly assigned to one of three conditions groups. We developed three questionnaires that only differed in levels of persona presentation in privacy intrusiveness. We refer to the different conditions as "data," "basic persona," and "advanced persona." The questionnaire opened with a description of a general scenario that the participants were asked to make decisions on as team members of a software company that develops applications. For both advanced and basic persona conditions, additional information referring to interviews held with end-users was shown. It was noted that the interviews had been designed to help the team develop a stronger understanding of end-users' behaviors and views on the new applications.

Next, five different mobile applications were randomly described to examine the study's dependent variable: privacy intrusiveness. The applications were chosen based on a pilot study based on Mechanical Turk (n=287), in which we eliminated applications that did not have sufficient variation in the privacy intrusiveness measure. The applications' names were invented, but we based the applications' functionalities on existing applications. The five applications used were 1) WeMail, which enables users to manage their emails; 2) Photo Album Creator, which enables users to create photo albums using photos stored on a device's memory card; 3) BiP, an online social network; 4) WeFit, which enables users to track their sport activities; and 5) Emoji Keyboard, which enables users to send messages with special emojis. For all of the conditions, the participants were presented with the application name, one screenshot, a short explanation of the application, and a sentence describing a particular case related to the application.

In designing the persona conditions, we were inspired by the definition of personas given in the literature [49]. For the basic and advanced persona conditions, the design was represented using a user's quote given under an invented end-user name. For the advanced persona condition, additional information on the end-user was presented, including a picture and a short description. It could be easily understood that the quotes and details referred to end-users who had been interviewed and who had been mentioned at the beginning. To minimize the differences between personas, thus avoiding biased answers based on the personas' details, they were all defined as undergrad females students from Tucson, AZ. Table 1 presents an example of Wefit, one of the hypothetic applications used. See our website link for phrasing used for all the scenarios and conditions [48].

The rest of the questionnaire elicited information on other independent variables. We referred to the participant's perceived levels of privacy. The participants were asked to contemplate the degrees of access that websites and apps have to their personal information and to answer several questions drawn from Dinev et al. [17]. Another personal aspect that we measured was that of empathy based on two of Davis' [15] four recommended empathy measurements: empathic concern and perspective taking. Finally, the questionnaire closed with demographic questions.

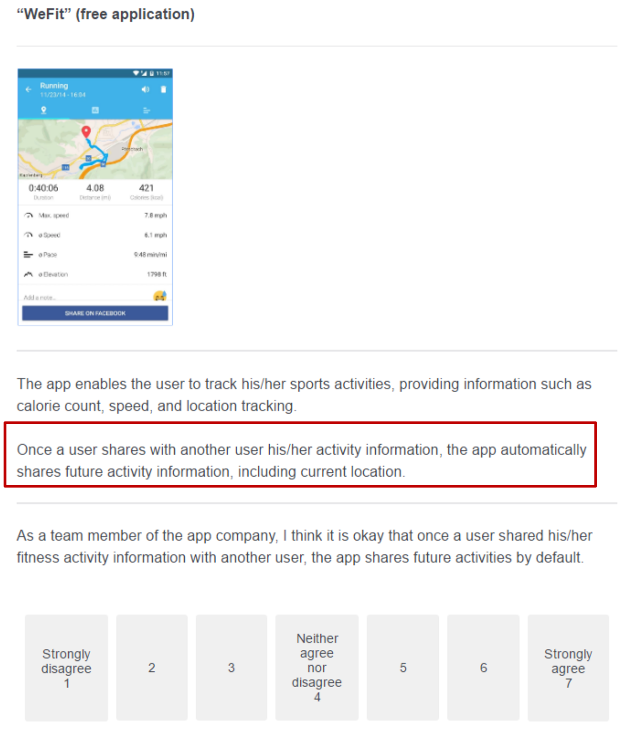
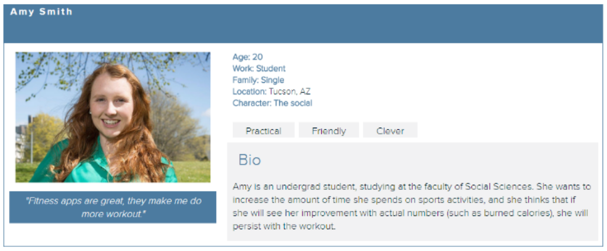
## 3.2. Recruitment

Former studies of the privacy field have used crowdsourcing methodologies to investigate different privacy aspects, including users' valuations of location privacy [47], users' privacy expectations of mobile apps [36] and crowdsourced recommendation system development for privacy protection settings used in popular apps [2]. For our purposes we recruited adult participants via AMT. Participants were required to be 18 years of age or older and to reside in the U.S. to ensure English proficiency. The study presentation did not include a mention of privacy to avoid biasing our participant base by attracting people who were more sensitive to privacy concerns [26].

Qualified participants followed a link that randomly assigned each participant to one of three links to the questionnaire. The questionnaire was built using the Qualtrics commercial web survey service. The participants completed an IRB-approved consent form on participation limitations. The questionnaire took approximately 6.5 min to complete, and our compensation rate was approximately $2.77 an hour, which is higher than the median hourly reservation wage [30, 44].

Following Goodman et al.'s [24] study on AMT, we phrased a question to identify participants who would not follow the survey's instructions [43]. The participants were presented with a reading comprehension test, which involved reading a short paragraph related to the survey content and answering

**Table 1. Measuring privacy intrusiveness using three conditions that differ in levels of persona presentation. For all of the conditions the mobile app's presentation opened with the presentation of the app's name and a screen shot followed by a description of a specific scenario. Then, a relevant decision-making question was asked. The conditions only differ in descriptions of the specific scenarios given (the outlined part).**

| Entire mobile app scenario presentation | Condition 1 – data display |
|---|---|
| <br>**"WeFit" (free application)**<br> Running<br>11/23/14 - 16:04<br>0:40:06<br>Duration<br>4.08<br>Distance (mi)<br>421<br>Calories (kcal)<br>Max. speed<br>7.8 mph<br>ø Speed<br>6.1 mph<br>ø Pace<br>9:48 min/mi<br>ø Elevation<br>1798 ft<br>Add a note...<br>SHARE ON FACEBOOK<br>The app enables the user to track his/her sports activities, providing information such as calorie count, speed, and location tracking.<br>Once a user shares with another user his/her activity information, the app automatically shares future activity information, including current location.<br>As a team member of the app company, I think it is okay that once a user shared his/her fitness activity information with another user, the app shares future activities by default.<br>Strongly disagree 1 · 2 · 3 · Neither agree nor disagree 4 · 5 · 6 · Strongly agree 7 | Once a user shares with another user his/her activity information, the app automatically shares future activity information, including current location. |
| | **Condition 2 – basic persona display**<br>Amy Smith, end-user: "Me and some of my friends downloaded the app. After finishing the first run, I shared with my friend, Julie, my running pace and all other measurements (average speed and etc.). A few days later, Julie surprised me with a bottle of juice at one point along my route. She explained that once I shared with another user my activity information, the app automatically shares future activity information, including current location." |
| | **Condition 3 – advanced personas display**<br>Amy Smith, end-user: "Me and some of my friends downloaded the app. After finishing the first run, I shared with my friend, Julie, my running pace and all other measurements (average speed and etc.). A few days later, Julie surprised me with a bottle of juice at one point along my route. She explained that once I shared with another user my activity information, the app automatically shares future activity information, including current location."<br><br>Amy Smith<br>"Fitness apps are great, they make me do more workout"<br>Age: 20<br>Work: Student<br>Family: Single<br>Location: Tucson, AZ<br>Character: The social<br> <br>Bio<br>Amy is an undergrad student, studying at the faculty of Social Sciences. She wants to increase the amount of time she spends on sports activities, and she thinks that if she will see her improvement with actual numbers (such as burned calories), she will persist with the workout. |

a question about it. We excluded participants' records if they answered the screening question incorrectly.

After filtering out participants who completed the screening task incorrectly, we removed 13 responses of the total 469. Concerning gender, two hundred thirty participants were female (50%), 224 were male (49%) and two participants did not reveal their gender (1%). The age distribution of our participants was as follows: 65 were between the ages of 18 and 24 (14%); 207 were between the ages of 25 and 34 (46%); 100 were between the ages of 35 and 44 (22%); 43 were between the ages of 45 and 54 (9%); 32 were between the ages of 55 and 64 (7%); and 9 were 65 or older (2%).

### 3.3. Data analysis

To ensure data validity, we used Cronbach's α measurement to determine the reliability [56] of each construct according to our designed questionnaire. Accordingly, we removed the item for the emoji keyboard scenario from the *privacy intrusive* measurement. Removing this item increased the Cronbach's α value from 0.75 to 0.76. The fact that this item decreased Cronbach's α value is not surprising, as the scenario was different in terms of context compared to other scenarios. The Emoji scenario described a privacy invasion that did not include any social aspect, unlike the other scenarios [48]. Similarly, we removed two items from the *perspective-taking* measurement that decreased the Cronbach's α value. See the Appendix for the results of the Cronbach's α test. Next, we performed a Herman single-factor test to control for the effects of Common Method Variance (CMV). A single factor explains 24% of the variance; therefore, our data are not exposed to CMV bias [46].

## 4. Results

### 4.1. Descriptive Statistics

We begin our analysis by reviewing the distributions of responses given on the questionnaire's main constructs. Figure 1 shows differences in the mean privacy intrusiveness scores among the presentation conditions. When persona presentations

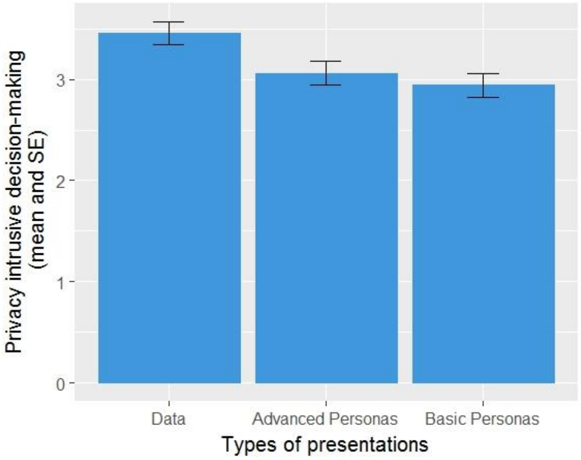


**Figure 1. Privacy intrusive decision making versus types of presentation based on the extent to which end-users' perspectives were emphasized.**

were used, decisions made were found to be less privacy intrusive. An ANOVA analysis shows a significant difference between the three conditions (F(2,453) = 5.34, p = 0.005). A post hoc t-test analysis shows a significant difference between the persona and data conditions (*p*-value: advanced vs. data: 0.018, basic vs. data: 0.002). The difference between the persona conditions was found to be insignificant. The data presentation mean privacy intrusiveness score was the highest (mean = 3.46, SE = 0.11), and the advanced and basic persona presentations received lower scores (advanced personas: mean = 3.06, SE = 0.12; basic personas: mean = 2.94, SE = 0.12).

## 4.2. Model validation

Next, we examined our hypotheses by conducting a regression analysis for predicting privacy intrusiveness. We used our proposed model and a stepwise technique to define the model and determine which predicting variables to include. The final regression consisted of six variables and latent variables (Table 2).

The regression model (adjusted $R^2 = 0.312$) pointed to two significant predictors affecting intrusive privacy decision-making: the level of persona presentations and the participants' perceived levels of privacy. We found that the existence of personas affected privacy intrusiveness in both basic and advanced persona conditions: (a) basic personas compared to data (β = -0.519, *p* < 0.001) and (b) advanced personas compared to data (β = -0.307, *p* = 0.03). The results show that the persona presentations spurred less privacy-intrusive decision-making, confirming our first hypothesis. We further analyzed the difference between advanced and basic persona presentation. We performed a regression through which advanced persona presentation was included in the overall variability (intercept), and we did not find a significant difference between types of persona presentation (advanced compared to basic: β = -0.212, *p* = 0.126). Our second hypothesis was also confirmed. We found that perceived privacy affects privacy intrusiveness in a contradictory direction compared to personas presentations and that it has a positive effect. The more the participant had a stronger perception of having privacy, the decision made was more privacy-intrusive.

**Table 2. Regression model predicting privacy intrusive decision making**
**Adjusted $R^2$ = 0.312, F (12,443) = 18.23, *p* < 0.001**

| | Estimated coefficient (β) | Std. Error | t value | Pr (>\|t\|) |
|---|---|---|---|---|
| (Intercept) | 2.554 | 0.397 | 6.427 | <0.001 |
| Perspective-taking | -0.031 | 0.066 | -0.477 | 0.633 |
| **Perceived privacy** | **0.469** | **0.035** | **13.241** | **<0.001** |
| Empathic concern | -0.097 | 0.059 | -1.656 | 0.098 |
| **Advan. personas** | **-0.307** | **0.141** | **-2.183** | **0.030** |
| **Basic personas** | **-0.519** | **0.138** | **-3.758** | **<0.001** |
| Gender: no answer | 0.889 | 0.865 | 1.027 | 0.305 |
| Gender: male | 0.067 | 0.119 | 0.560 | 0.576 |
| Age: 25-34 | -0.090 | 0.172 | -0.521 | 0.602 |
| Age: 35-44 | -0.177 | 0.195 | -0.909 | 0.364 |
| Age: 45-54 | -0.151 | 0.242 | -0.625 | 0.533 |
| Age: 55-64 | 0.004 | 0.265 | 0.014 | 0.989 |
| Age: 65+ | -0.806 | 0.435 | -1.852 | 0.065 |

Other latent variables were found to be non-significant and were used as our control. We found that both constructs representing personal empathic elements, empathic concern, and perspective taking did not have a significant effect on privacy intrusiveness. Effects thus resulted from increasing empathy through persona presentation and not as a result of being more empathic in general. Finally, both age and gender were found to be non-significant variables.

# 5. Discussion

## 5.1. Theoretical Implications

There is an ongoing debate about the ability of personas to evoke empathy towards end-users. Encouraging empathy is one of the fundamental goals of personas and guides the designers to consider end-users' perspectives [49]. Previous studies have reported conflicting results regarding the ability of personas to positively affect empathy (see Nielsen [42] versus Friess [23]). Our findings, which were obtained in the field of privacy, contribute to this general discussion by providing empirical results that support the existence of the positive impact of personas on increasing empathy.

Our experimental design rules out the possibility that privacy intrusiveness is linked to user experience outcomes. The experimental conditions differ in the framing of the described scenarios. A “dry” description not referring to the end-user’s perspective led to a decision that was up to 15% more favorable from a commercial point of view. Citing a “real” person with a name and a short story caused people to design systems that were more in line with the end-users’ goals and experiences. We also examined whether personal empathy affects privacy intrusiveness, similar to Detert et al. [16], who explored the indirect impacts of empathy on ethical decision making. In our case, we did not find a significant impact of empathy on privacy intrusiveness. Thus, the results highlight the effects of the framing of persona design on the reduction of privacy intrusiveness. The framing does not necessarily need to be complicated. Our results show that even basic personas through which the design was presented from the point of view of a named user have an effect on decisions.

The effect of personal perceived privacy on privacy intrusiveness was also explored. We would expect users who consider their privacy as more protected to be more keen to take risks with systems that are more intrusive. We attribute this finding to the trust that they felt toward information systems they thought of while answering relevant questions.

The initial objective of user-centered design (UCD) was to increase product usability [45]. The concept was later broadened to other end-users’ aspects, including their enjoyment of a product and willingness to use it [29]. Other scholars have argued for the application of privacy and trust [33] and security [60] as usability goals. We believe that UCD can – and should – be extended to address privacy concerns. Mounting evidence points to the role that privacy plays in customers’ choices. For instance, an online social network is only one example of an information system that is used continuously by end-users. Therefore, when decision makers consider only a website’s or app’s usability but ignore the risks related to information flows and when decision maker collect unnecessary personal information, they are failing to apply a critical long-term usability goal.

## 5.2. Design Implications

Our results suggest the potential of extending the privacy-by-design methodology with UCD concepts, especially with personas. Although user involvement was noted in some Privacy Impact Assessments guidelines, it was not clear how to conduct such involvement. Our findings create the foundations for an assistive tool to be used by developers and other privacy decision-makers. The use of personas allowed us to frame the presented problem within the context of end-users, facilitating a more privacy-sensitive critique. We argue that this critique better reflects the users’ actual behaviors, given the intrusive nature of the scenarios.

Our findings exemplify how consulting directly with users can lead to a concrete implementation of Value Sensitive Design (VSD), which is described as “a theoretically grounded approach to the design of technology that accounts for human values in a principled and comprehensive manner throughout the design process.” [22] PbD can be thought of as an instance of VSD, in which privacy is the human value that we wish to promote. Our results suggest that personas can lead to more sensitivity to privacy without forcing participants to apply one point of view or another. The framing itself supports a more emphatic understanding of users’ experiences embedded in scenarios. This means that using personas might not necessarily promote privacy in every case but will promote closer and more reliable feedback on design artifacts. Examining design issues from the end-users' point of view has the potential to change design outcomes to be better aligned with the long-term needs and goals of users.

The implementation of specific aspects related to PbD will soon become mandatory for many companies with the enforcement of European Union GDPR (article 23, [20]). Although the use of PbD can promote privacy, our results point to possible shortcomings in its current form. Specifically, our findings support the criticisms of Koops et al. [32], which point to the difficulties of asking developers to remain faithful to a single (“hardcoded”) set of design principles, as this single pattern may not be able to support delicate contexts of privacy. Instead, a focus should be placed on incorporating design feedback from users (and other stakeholders) to “internalize the data protection framework as part of their mindset.” [32] Moreover, our results point to the dangers of relying on data flow analyses when making privacy design decisions. PIAs, as a crucial facet of PbD, rely heavily on describing and analyzing data flows. However, our findings show that decisions based on data flows from a systems perspective and without considering the implications from end-user perspectives may be more privacy intrusive. Thus, despite their intentions to promote privacy, this may make PIA methods harmful.

Personas can augment several stages of the privacy-by-design processes. Analyzing and personifying users and their relations to data privacy can be used as a first step to applying a more humanized approach to privacy-by-design. We found that framing scenarios with a human aspect supported a 15% increase in the perception of privacy intrusiveness. Developers could, in turn, use humanized framing for future information systems design when turning to the general population and when soliciting their privacy design critiques. Personas can also serve as a basis for understanding the sensitivity of data to various archetypes of users and to different modes of consent, control, and recourse. Personas are also used to facilitate communication between designers and other stakeholders on end-users' goals, needs, and beliefs.

### 5.3. Limitations and Future Work

Our study is subject to several limitations that impact its applicability for design and research. First, we did not limit the crowd used to specific workers who may be relevant to a specific application. Future studies might test the capacities to locate specific types of crowd workers. Second, we only examined privacy violations that are visible and detectable by users. Data uses that occur in the background are not under the study's scope. Third, concerning the study's dependent measurements, we used the same direction in all scenarios, in which choosing a lower score (from 1 to 7) represented a less privacy-intrusive decision. Finally, for the advanced personas condition, we made an effort to use representative users who were as similar as possible. However, there is still a chance that the participants answered in a certain way due to considerations referring to a particular persona's details. As the SE of the mean of the advanced persona score is similar to that of the two other conditions, we can assume that even if this did occur, it did not occur in most cases.

The current study investigated if and how the framing of design scenarios affects privacy design decisions. It will be interesting to continue on to further studies on personas themselves to see how differences between them can affect privacy design decisions. Rather than trying to create personas that are as similar as possible, which was essential for our study, several possible directions could be applied and manipulated to limit privacy intrusiveness or another dependent variable. Furthermore, future studies may investigate how using different user personas affects design decisions, such as users who feel they have nothing to hide [55] or privacy fundamentals.

## 6. Conclusions

This paper investigates privacy design critiques under the normative assumption of promoting privacy-respectful system design. Our study explores how personas, which are typically used to help designers analyze and capture end-users' experiences, can actually deliver a more emphatic design critique. Using an online experimental design (n = 456), we found that framing privacy design dilemmas based on end-users' perspectives and not solely as a matter of "data" limits the extent to which decisions made are privacy intrusive. We compared the experiment's conditions based on ascending levels of persona presentation and found that the existence of personas resulted in lower levels of privacy intrusiveness. We think that a possible explanation for our result is the evocation of empathy toward the end-users as a consequence of the persona presentations.

The findings reported in this paper have several implications for questions related privacy-by-design and user-centered design. First, we confirm our hypothesis on the use of personas and on their effects on privacy intrusiveness, opening up a design space for tools that use personas to enhance privacy in the development process. Second, the findings extend the conceptualization of usability and highlight new ways to explore similar relationships between personas and other ethical issues.

## 7. References

[1] Abras, C., Maloney-Krichmar, D. and Preece, J. 2004. User-centered design. *Bainbridge, W. Encyclopedia of Human-Computer Interaction. Thousand Oaks: Sage Publications*. (2004), 37(4), 445-456.

[2] Agarwal, Y. and Hall, M. 2013. ProtectMyPrivacy : Detecting and Mitigating Privacy Leaks on iOS Devices Using Crowdsourcing Categories and Subject Descriptors. *Proceeding of the 11th annual international conference on Mobile systems, applications, and services* (2013), 97–110.

[3] Arad, A. and Rubinstein, A. 2015. The People's Perspective on Libertarian--Paternalistic Policies. Unpublished Manuscript.

[4] Ayalon, O., Toch, E., Hadar, I. and Birnhack, M. 2017. How Developers Make Design Decisions about Users' Privacy: The Place of Professional Communities and Organizational Climate. *Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing - CSCW '17 Companion*. (2017), 135–138.

[5] Balebako, R., Marsh, A., Lin, J., Hong, J.I. and Cranor, L.F. 2014. The Privacy and Security Behaviors of Smartphone App Developers. *Workshop on Usable Security (USEC)*. (2014).

[6] Bamberger, K.A. and Mulligan, D.K. 2011. *Privacy on the Books and on the Ground.*

[7] Birnhack, M., Toch, E. and Hadar, I. 2014. Privacy mindset, technological mindset. *Jurimetrics: Journal of*

*Loaw, Science & Technology*. 55, June (2014), 1–71.

[8] Blomquist, Å. and Arvola, M. 2002. Personas in Action : Ethnography in an Interaction Design Team. *Proceedings of the second Nordic conference on Human-computer interaction* (2002), 197–200.

[9] Boyd, D. 2010. Making Sense of Privacy and Publicity. *South by Southwest (SXSW 2010)–transcription of the talk*.

[10] Cavoukian, A. 2009. Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario, Canada.

[11] Chai, P.R., Ranney, M.L., Boyer, E.W., Rosen, R.K. and Lewis, D.M. 2017. Crowd-Sourced Focus Groups on Twitter : 140 Characters of Research Insight. *Proceedings of the 50th Hawaii International Conference on System Sciences* (2017).

[12] Chang, C.T. and Lee, Y.K. 2009. Framing charity advertising: Influences of message framing, image valence, and temporal framing on a charitable appeal. *Journal of Applied Social Psychology*. 39, 12 (2009), 2910–2935.

[13] Cooper, A. 2004. *The inmates are running the asylum:[Why high-tech products drive us crazy and how to restore the sanity]*. Sams.

[14] Dandavate, U., Sanders, E.B.N. and Stuart, S. 1996. Emotions matter: User empathy in the product development process. *The Human Factors and Ergonomics Society Annual Meeting* (1996), Vol. 40, No. 7, pp. 415–418.

[15] Davis, M.H. 1980. *A Mulitdimensional Approach to Individual Differences in Empathy*.

[16] Detert, J.R., Treviño, L.K. and Sweitzer, V.L. 2008. Moral disengagement in ethical decision making: A study of antecedents and outcomes. *Journal of Applied Psychology*. 93, 2 (2008), 374–391.

[17] Dinev, T., Xu, H., Smith, J.H. and Hart, P. 2012. Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*. 22, 3 (2012), 295–316.

[18] Dow, S., Gerber, E. and Wong, A. 2013. A pilot study of using crowds in the classroom. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2013).

[19] Egelman, S., Felt, A.P. and Wagner, D. 2013. Choice architecture and smartphone privacy: There's a price for that. *The Economics of Information Security and Privacy*. (2013), 211–236.

[20] EUGDPR: 2017. *http://www.eugdpr.org/article-summaries.html*.

[21] Felt, A.P., Egelman, S. and Wagner, D. 2012. I've got 99 problems, but vibration ain't one. *Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices - SPSM '12*. (2012), 33.

[22] Friedman, B. 1996. Value-sensitive design. *interactions*. 3, 6 (1996), 16–23.

[23] Friess, E. 2012. Personas and decision making in the design process: an ethnographic case study. *Conference on Huma*. April (2012), 1209–1218.

[24] Goodman, J.K., Cryder, C.E. and Cheema, A. 2013. Data Collection in a Flat World: The Strengths and Weaknesses of Mechanical Turk Samples. *Journal of Behavioral Decision Making*. 26, 3 (2013), 213–224.

[25] Gray, C.M. 2016. "It's More of a Mindset Than a Method." *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16* (2016).

[26] Gross, R. and Acquisti, A. 2005. Information revelation and privacy in online social networks. *Proceedings of the 2005 ACM workshop on Privacy in the electronic society* (2005), 71–81.

[27] Gürses, S., Troncoso, C. and Diaz, C. 2011. Engineering privacy by design. *Computers, Privacy & Data Protection*. 14, no. 3, (2011).

[28] Hadar, I., Hasson, T., Ayalon, O., Toch, E., Birnhack, M., Sherman, S. and Balissa, A. 2017. Privacy by designers: software developers' privacy mindset. *Empirical Software Engineering*. (2017), 1–31.

[29] Hanington, B. 2003. Methods in the Making: A Perspective on the State of Human Research in Design. *Design Issues*. 19, 4 (2003), 9–18.

[30] Horton, J. and Chilton, L. 2010. The Labor Economics of Paid Crowdsourcing. *Proceedings of the 11th ACM conference on Electronic commerce* (2010), 209–218.

[31] ICO (Information Commissioner's Office) 2014. Conducting privacy impact assessments code of practice. *Ico.Org.Uk*. (2014), 1–55.

[32] Koops, B.-J. and Leenes, R. 2014. Privacy regulation cannot be hardcoded. A critical comment on the "privacy by design" provision in data-protection law. *International Review of Law, Computers & Technology*. 28, 2 (2014), 159–171.

[33] Kramer, J., Noronha, S. and Vergo, J. 2000. A user-centered design approach to Personalization. *Communications of the ACM*. 43, 8 (2000), 45–48.

[34] Langheinrich, M. 2001. Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. *3rd international conference on Ubiquitous Computing*. (2001), 273–291.

[35] Lewis, M.M. and Coles-Kemp, L. 2014. Who says personas can't dance?: the use of comic strips to design information security personas. *CHI '14 Extended Abstracts on Human Factors in Computing Systems* (2014).

[36] Lin, J., Sadeh, N., Amini, S., Lindqvist, J., Hong, J.I. and Zhang, J. 2012. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. *Proceedings of the 2012 ACM Conference on Ubiquitous Computing - UbiComp '12*. (2012), 501.

[37] Luther, K., Pavel, A., Wu, W., Tolentino, J., Agrawala, M., Hartmann, B. and Dow, S.P. 2014. CrowdCrit. *Proceedings of the companion publication of the 17th ACM conference on Computer supported cooperative work & social computing - CSCW Companion '14*. (2014), 21–24.

[38] Massanari, A.L. 2010. Designing for imaginary friends: information architecture, personas and the politics of user-centered design. *New Media & Society*. 12, 3 (2010), 401–416.

[39] Mattelmäki, T. and Battarbee, K. 2002. Empathy Probes. *Pdc*. June (2002), 266–271.

[40] Miaskiewicz, T., Grant, S.J., Kozar, K.A. and Grant, S.J. 2009. A Preliminary Examination of Using Personas to Enhance User-Centered Design. (2009).

[41] Mulder, S. and Yaar, Z. 2006. *The user is always right: A practical guide to creating and using personas for the web*. New Riders.

[42] Nielsen, L. and Storgaard Hansen, K. 2014. Personas is applicable: a study on the use of personas in Denmark. *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*. (2014), 1665–1674.

[43] Oppenheimer, D.M., Meyvis, T. and Davidenko, N. 2009. Instructional manipulation checks: Detecting satisficing to increase statistical power. *Journal of Experimental Social Psychology*. 45, 4 (2009), 867–872.

[44] Paolacci, G., Chandler, J. and Ipeirotis, P. 2010. Running experiments on amazon mechanical turk. *Judgment and Decision making*. 5, 5 (2010), 411–419.

[45] Pea, R.D. 1987. User Centered System Design: New Perspectives on Human-Computer Interaction. *Journal educational computing research*. 3, 1 (1987), 129–134.

[46] Podsakoff, P.M. 1986. Self-Reports in Organizational Research: Problems and Prospects. *Journal of Management*. 12, 4 (1986), 531–544.

[47] Poikela, M. and Toch, E. 2017. Understanding the Valuation of Location Privacy: a Crowdsourcing-Based Approach. *Proceedings of the 50th Annual Hawaii International Conference on System Sciences*. (2017).

[48] Privacy intrusiveness measurements: 2017. *https://www.oshratayalon.com/hicss-appendeix*.

[49] Pruitt, J. and Adlin, T. 2010. *The persona lifecycle: keeping people in mind throughout product design*. Morgan Kaufmann.

[50] van Rest, J., Boonstra, D., Everts, M., van Rijn, M. and van Paassen, R. 2012. Designing privacy-by-design. *Annual Privacy Forum* (2012), 55–72.

[51] Robb, D.A., Padilla, S., Kalkreuter, B. and Chantler, M.J. 2015. Crowdsourced Feedback With Imagery Rather Than Text: Would Designers Use It? *Proceedings of the ACM CHI'15 Conference on Human Factors in Computing Systems*. 1, (2015), 1355–1364.

[52] Rode, J., Le Menestrel, M. and Cornelissen, G. 2015. Can monetary valuation undermine nature conservation? Evidence from a decision experiment. (2015).

[53] Rubinstein, A. 2006. A sceptic's comment on the study of economics. *Economic Journal*. 116, 510 (2006), 1–9.

[54] Rubinstein, I.S. and Good, N. 2013. Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents. *Berkeley Technology Law Journal*. 28, 2 (2013), 1333–1413.

[55] Spears, J.L. and Erete, S.L. 2014. " I have nothing to hide ; thus nothing to fear ": Defining a Framework for Examining the " Nothing to Hide " Persona. *Symposium on Usable Privacy and Security*. (2014), 1–5.

[56] Straub, D., Boudreau, M.-C. and Gefen, D. 2004. Validation Guidelines for Is Positivist. *Communications of the Association for Information Systems*. 13, 24 (2004), 380–427.

[57] Tversky, A. and Kahneman, D. 1981. The framing of decisions and the psychology of choice. *Science*. 211, 4481 (1981), 453–458.

[58] Wright, D. 2012. The state of the art in privacy impact assessment. *Computer Law & Security Review*. 28(1), (2012), 54–61.

[59] Xu, A., Huang, S. and Bailey, B. 2014. Voyant: Generating Structured Feedback on Visual Designs Using a Crowd of Non-Experts. *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing - CSCW '14*. (2014), 1433–1444.

[60] Zurko, M.E. and Simon, R.T. 1996. User-centered security. *Proceedings of the 1996 workshop on New security paradigms - NSPW '96* (1996), 27–33.

[61] Federal Trade Commission. 2012. Protecting consumer privacy in an era of rapid change. FTC report.

# Appendix

## Final Cronbach's α tests' results

| Construct | Number of items | Cronbach's α |
|---|---|---|
| Privacy intrusiveness | 4 | 0.76 |
| Perceived privacy | 3 | 0.92 |
| Empathic concern | 7 | 0.88 |
| Perspective taking | 5 | 0.80 |