Transparency of Privacy Risks Using PIA Visualizations

Ala Sarah Alaqra[1](✉), Simone Fischer-Hübner[1,2], and Farzaneh Karegar[1]

[1] Karlstad University, Karlstad, Sweden
as.alaqra@kau.se
[2] Chalmers University of Technology, Gothenburg, Sweden
http://www.springer.com/gp/computer-science/lncs

Abstract. Privacy enhancing technologies allow the minimization of risks to online data. However, the transparency of the minimization process is not so clear to all types of end users. Privacy Impact Assessments (PIAs) is a standardized tool that identifies and assesses privacy risks associated with the use of a system. In this work, we used the results of the PIA conducted in our use case to visualize privacy risks to end users in the form of User Interface (UI) mock ups. We tested and evaluated the UI mock-ups via walkthroughs to investigate users' interests by observing their clicking behavior, followed by four focus group workshops. There were 13 participants (two expert groups and two lay user groups) in total. Results reveal general interests in the transparency provided by showing the risks reductions. Generally, although participants appreciate the concept of having detailed information provided about risk reductions and the type of risks, the visualization and usability of the PIA UIs require future development. Specifically, it should be tailored to the target group's mental models and background knowledge.

Keywords: Privacy Impact Assessment · User Interface · Usability · Transparency · Privacy-Enhancing Technologies

1 Introduction

Personal data analysis based on Machine Learning is increasingly used, e.g. for enabling new eHealth services or for commercial applications, but may result in privacy risks for the individuals concerned (specifically data subjects). Consequently, there is a need to develop and use Privacy-Enhancing Technologies (PETs) to mitigate privacy risks. PETs can support users' privacy and data protection by enforcing the legal privacy principles of, for example, data minimization through anonymization or pseudonymization of personal data [15]. There are several data minimization PETs, including homomorphic encryption (HE) and Functional Encryption (FE) schemes for data analyses as well as differential privacy for federated learning [5,6]. The above-mentioned PETs were developed

A. Moallem (Ed.): HCII 2023, LNCS 14045, pp. 3–17, 2023.
https://doi.org/10.1007/978-3-031-35822-7_1

and demonstrated in the PAPAYA Horizon 2020 EU project[1]. PAPAYA stands for PlAtform for PrivAcY preserving data Analytics.

Given the approaches of different PETs for minimizing risks to one's online data, the use of PETs, however, cannot guarantee absolute risk abolition in practice. This study investigates the transparency and communication of Functional Encryption (FE) risk reductions. Through user interface (UI) visualizations of the conducted Privacy Impact Assessment (PIA) for FE, we investigate users' perspectives of the PIA elements. We take into consideration users' technical knowledge (lay and expert users) and further report on recommendations for future PIA visualizations and designs.

1.1 Objective and Research Questions

The purpose of this study is to evaluate user interface mock-ups explaining how privacy-preserving data analysis is working with the PAPAYA platforms developed in the project. Therefore, the following are the research questions of this study:

> RQ1: What are the users' (experts and lay) perceptions of the visualizations of PIA risks in a user interface?
> RQ2: What are the recommendations for future UI visualization implementations of usable PIAs?

1.2 Outline

In the following section (Sect. 2), we present the background and related work to this study as well as the UI mock-ups of the PIA of the use case used in this study. In Sect. 3 we describe the methodology and study design. Results are presented in Sect. 4. Derived recommendations for the UI visualizations are discussed in Sect. 5. Finally, our conclusions are found in Sect. 6.

2 Background and Related Work

We present the background and related work to our study in the following subsections. That includes the use case scenario used as well as work on the PIA user interfaces.

2.1 Privacy Impact Assessment

For assessing the extent and type of privacy risks of data processing practices a Privacy Impact Assessment can be conducted [11].

A PIA is used to evaluate the potential privacy risks associated with a system and could be defined as "a process whereby the potential impacts and implications of proposals that involve potential privacy-invasiveness are surfaced and

[1] https://www.papaya-project.eu/.

examined" [10]. According to [11], a PIA's definition has evolved throughout time and the specification varies depending on the jurisdiction.

The EU General Data Protection Regulation (GDPR) requires data controllers to conduct a PIA for applications which are likely to result in high privacy risk [13]. A PIA can help communicate how the PETs in place reduce privacy risks, which contributes to improving users' trust and their willingness to share their data. Furthermore, previous research has shown users' existing interest in knowing about the underlying PETs in place (i.e., how PETs protect their data and the potentially remaining risks despite PETs used), which can help them in making informed privacy decisions [2,16]. Consequently, for enhancing transparency for different stakeholders, including end users, our objective is to explore how and to what extent we should explain to stakeholders how the PETs in place can reduce their privacy risks with a focus on communicating the results of PIA.

While a PIA is needed for complying with regulations, especially in the case of data analyses of medical data, we see an opportunity of using PIAs also as a means to inform different stakeholders of how PETs can reduce privacy risks. Promising results of a previous study show that the stakeholders appreciated and had more trust in the PET– a privacy-enhancing data analytics platform enabling medical data analyses on homomorphically encrypted patient data– by the mere fact that the service provider has conducted and displayed results of the PIA [3].

However, details and visualization of specific elements of the PIA were requested by participants of the study conducted in [3]. Furthermore, participants requested information about the PET method (incl. information on how Homomorphic Encryption (HE) works), the PIA method and how it was conducted, and the qualification of the individuals that conducted the PIA [2].

2.2 PETs and Transparency

Functional encryption is an encryption mechanism enabling an authorized party, which has the functional decryption key (a.k.a. evaluation key), to compute and learn an authorized function of the encrypted data (see also [4]). In contrast to homomorphic encryption, the result of the computed function is not encrypted meaning that the authorized party gets the result of the computation in an unencrypted form.

Transparency is a legal privacy principle (pursuant to Art.5 (1), 12 GDPR) and usable transparency concerning privacy-enhancing technologies can be a means for enhancing trust in those technologies (see e.g. [7,18]).

However, providing transparency of PETs in a usable manner poses several challenges. For instance, our previous studies on metaphors for illustrating PETs and making their privacy functionality transparent revealed misconceptions that users have, also for the reason that users may assume that a PET would be functioning in a similar way as security technologies that they are familiar with and would thus have comparable security properties [2,3,16]. Commonly used metaphors (such as the metaphors often used for explaining differential privacy i.e., the pixelation of photos) may also rather provide a structural explanation for a PET, while recent research has shown that functional explanations of privacy and security technologies are better understandable for end users [12].

Therefore, higher emphasis should be put on functional explanations, and explaining how PETs can reduce privacy risks via PIA illustrations can be one usable form of such a functional explanation. Such PIA illustrations should also provide guidance on adequate (residual) risks per context and what this implies (as suggested in [16,19]).

2.3 Use Case Scenario and Visualizations for Users

We utilized a specific commercial use case for the PAPAYA project involving data analyses for functionally encrypted data. The PIA results were produced with an extended version of the PIA tool by the French Data Protection Agency CNIL [1]). While the CNIL PIA focuses on assessing and displaying risks in terms of the classical security goals of Confidentiality, Integrity and Availability, an extended PIA tool version was developed in the PAPAYA project [14] (and is in the rest of this paper referred to as the "PAPAYA tool"). The PAPAYA tool, in addition, assesses and displays privacy risks in terms of the privacy goals of data minimization, intervenability and transparency and shows how they can be reduced by the use of a PET.

Moreover, the enhanced tool produced graphical output of the assessed risks and risk reductions for mobile devices, i.e., with limited screen sizes. The graphical output of the assessed risks by the enhanced tool was used in the design of the UI mock-ups of the study reported in this paper. We displayed the results of the PIA as a part of multi-layered structured consent forms of the use case in which we provided more details about the PET. Table 1 displays the list of the risks, the corresponding name of the risk in the UI, and descriptions.

In the use case, a Telecom provider called TelecomAB offers a service in their application. In their service, app users are prompted with a consent form asking if they would participate and contribute their personal usage data for a statistical survey study. The UI shows a declaration that the data should be protected by PAPAYA's Privacy by Design approach and offers details in the UI mock-ups.

Figure 1 gives an overview of the UI mock-up figures presented in this paper. The UI mock-ups present the consent form for participating data for a study by TelecomAB (Fig. 2a), information about PIA and Privacy by design (Fig. 2b and 2c), and the risk reductions and illustrations (Figs. 2d, 3a, and 3b).

2.4 PIA User Interfaces

In Fig. 2a, the UI illustrates the screen where the consent, for contributing one's data to a study, is presented to end users. In this UI, we show the consent prompt for users to contribute their specified data with MediaSurvey Corporation on behalf of TeleComAB (the data controller). In return, users would receive a monetary incentive of a five-euro voucher in this case. Further, we show that

Table 1. List of Privacy/Security aspects at risk and the corresponding name and description of the risk in the UI

Aspect at risk	Name of risk in UI	Description of remaining risks
Confidentiality	Illegitimate Data Access	The risk seriousness and likelihood that TeleComAB could access your data (age and social network usage) are reduced from 'Important' to 'Negligible'
Integrity	Unwanted Modification of Data	The risk seriousness that data could be falsified is reduced from 'Important' to 'Limited' while the risk likelihood is reduced from 'Important' to 'Negligible'
Availability	Data Disappearance	The risk seriousness that data could be lost is reduced from 'Important' to 'Limited' while the risk likelihood is reduced from 'Important' to 'Negligible'
Transparency	Intransparent Data Processing	The risk seriousness and likelihood that the data processing is not made transparent to the users is reduced from 'Important' to 'Limited'
Unlinkability	Linkable Data Processing potentially identifying users	The risk seriousness that TeleComAB could identify users and their social network usage profile based on the provided data is from 'Maximum' to 'Negligible', while the risk likelihood is reduced to reduced from 'Important' to 'Negligible'. There are small (negligible) risks remaining that personal data could be inferred from the calculated statistics
Intervenability	Lack of User Control	Not impacted. As TeleComAB cannot identify the users (data subjects), TeleComAB is not obliged to allow users to exercise their data subject rights according to Art 11 GDPR

data would be aggregated and securely encoded as well as the purpose for using the specified data (age, ad social network usage in this use case scenario). Here we provide a link to TeleComAB's PIA and Privacy by Design (PbD) approach presented in Fig. 2b.

We present information about the PIA and PbD approach in the UI of Fig. 2b. Regarding the PbD, TeleComAB state that "Our **Privacy by Design** approach ensures that your data will only be sent to us and statistically analysed by us in aggregated and securely encoded form. We will not be able to decode your data and can only derive statistics from your and other user's data". Reasons for conducting the PIA are illustrated under "Why did we conduct a PIA" UI

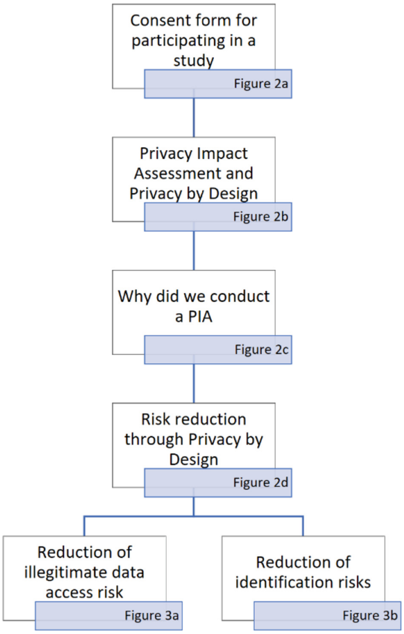
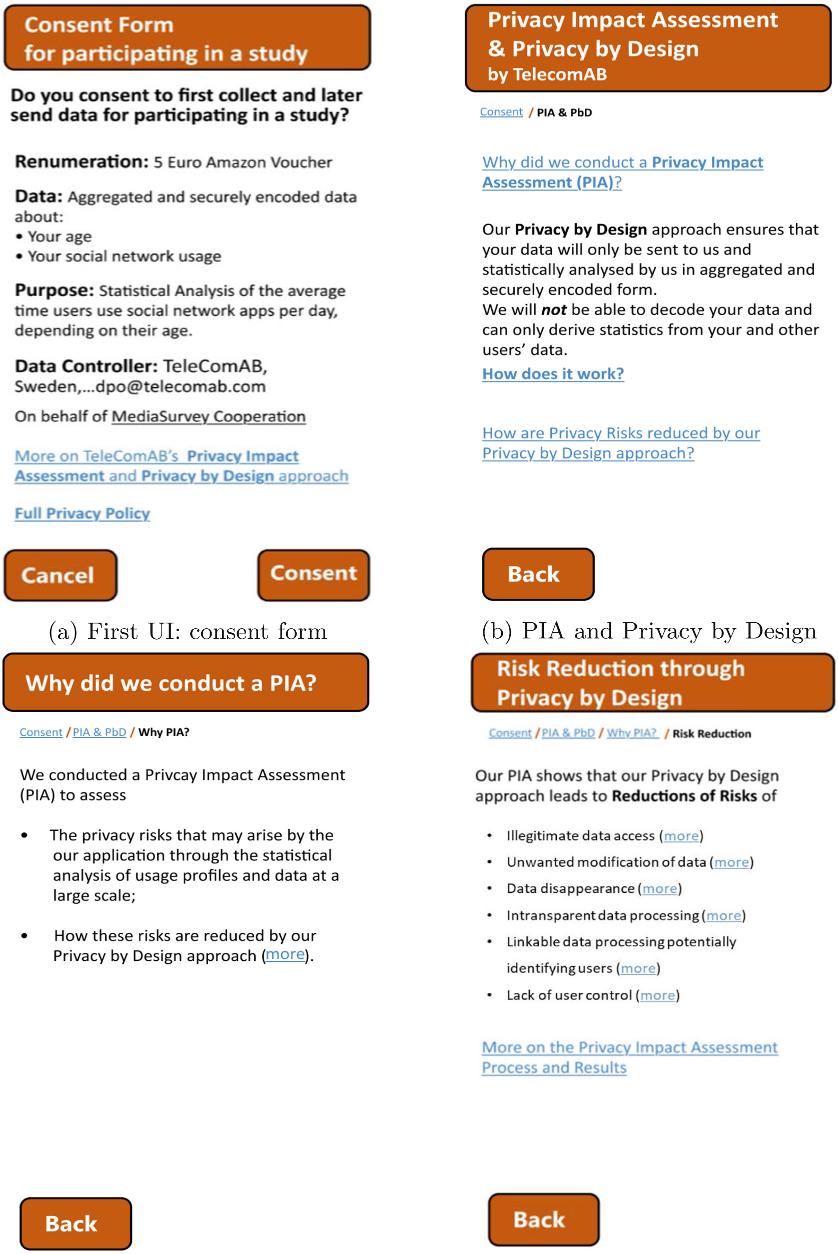

Consent form for participating in a study
Figure 2a
Privacy Impact Assessment and Privacy by Design
Figure 2b
Why did we conduct a PIA
Figure 2c
Risk reduction through Privacy by Design
Figure 2d
Reduction of illegitimate data access risk
Figure 3a
Reduction of identification risks
Figure 3b

Fig. 1. Overview of mock-up UI figures

(Fig. 2c. We show that there are privacy risks for sharing the data in this scenario and how these risks are reduced by the PbD approach. An overview of the PIA results showing the list of risks reduced by the PbD approach is illustrated in Fig. 3a. Details and visual illustrations of specific risk reductions are shown in Figs. 3a and 3b.

In Fig. 3a, the user interface shows a risk heat map with an overview of reductions of risks based on the PIA, in addition to the details about the specific risks (clicking the 'more' link). For instance, in Fig. 3a, the visualization of the illegitimate data access risk is shown. It shows that both risk seriousness and risk likelihood are reduced from serious to negligible. Further details relating to specific data (age and social network usage) as well as actors (TeleComAB) accompanied the visualization of risks relating to the use case. Similarly, in Fig. 3a, the UI illustrates the reduction of identification risks associated with participating/sharing their data in the scenario. We further present remaining negligible risks entailing possible inference of personal data from the calculated statistics results.



Consent Form
for participating in a study

Do you consent to first collect and later send data for participating in a study?

Renumeration: 5 Euro Amazon Voucher

Data: Aggregated and securely encoded data about:
- Your age
- Your social network usage

Purpose: Statistical Analysis of the average time users use social network apps per day, depending on their age.

Data Controller: TeleComAB, Sweden,...dpo@telecomab.com

On behalf of MediaSurvey Cooperation

More on TeleComAB's **Privacy Impact Assessment** and **Privacy by Design** approach

Full Privacy Policy

(a) First UI: consent form

Privacy Impact Assessment
& Privacy by Design
by TelecomAB

Consent / **PIA & PbD**

Why did we conduct a **Privacy Impact Assessment (PIA)**?

Our **Privacy by Design** approach ensures that your data will only be sent to us and statistically analysed by us in aggregated and securely encoded form.
We will ***not*** be able to decode your data and can only derive statistics from your and other users' data.

How does it work?

How are Privacy Risks reduced by our Privacy by Design approach?

(b) PIA and Privacy by Design

Why did we conduct a PIA?

Consent / PIA & PbD / **Why PIA?**

We conducted a Privcay Impact Assessment (PIA) to assess

- The privacy risks that may arise by the our application through the statistical analysis of usage profiles and data at a large scale;
- How these risks are reduced by our Privacy by Design approach (more).

(c) PIA: Why

Risk Reduction through
Privacy by Design

Consent / PIA & PbD / Why PIA? / **Risk Reduction**

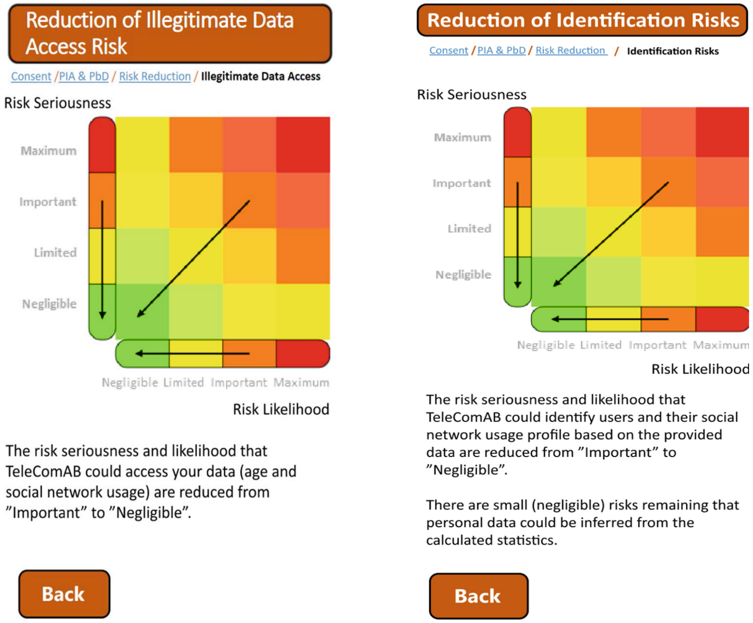
Our PIA shows that our Privacy by Design approach leads to **Reductions of Risks** of

- Illegitimate data access (more)
- Unwanted modification of data (more)
- Data disappearance (more)
- Intransparent data processing (more)
- Linkable data processing potentially identifying users (more)
- Lack of user control (more)

More on the Privacy Impact Assessment Process and Results

(d) Overview of risk reductions

Fig. 2. Overview of the use case UIs


Reduction of Illegitimate Data Access Risk
Consent / PIA & PbD / Risk Reduction / Illegitimate Data Access
Risk Seriousness
Maximum
Important
Limited
Negligible
Negligible Limited Important Maximum
Risk Likelihood
Back
Reduction of Identification Risks
Consent / PIA & PbD / Risk Reduction / Identification Risks
Risk Seriousness
Maximum
Important
Limited
Negligible
Negligible Limited Important Maximum
Risk Likelihood
Back

The risk seriousness and likelihood that TeleComAB could access your data (age and social network usage) are reduced from ”Important” to ”Negligible”.

The risk seriousness and likelihood that TeleComAB could identify users and their social network usage profile based on the provided data are reduced from ”Important” to ”Negligible”.

There are small (negligible) risks remaining that personal data could be inferred from the calculated statistics.

(a) Illegitimate data access risk (b) Identification risks

Fig. 3. Risks reduction UIs

3 Methodology

The PAPAYA project followed a PbD approach [8,9], where we focus and take privacy considerations in the early stages of the development process of the project's PETs. As our objective is to investigate how to communicate/make transparent the PIA results to users, we, therefore, designed UI mock-ups to display PIAs risks and visualize each risk mitigation for our use case (found in Sect. 2.4). Based on the UI mock-ups we conducted the user studies as described below.

3.1 Study Design

The method used in this study is two-fold. First, we had individual walkthroughs of the UI mock-ups. Second, we had four focus group workshops with 3–4 participants in each. All studies were conducted online due to COVID19 restrictions at the time. We used Zoom (a video conferencing service) and Mentimeter (an interactive presentation software) to remotely facilitate the interactions and discussions of the studies. Participants were asked to share their screens for the UI walkthroughs as they clicked around the interactive UI mock-up. After consenting to participate in the study, participants were also asked to consent to the screen recording and the voice recording of the sessions.

In total, there were 13 participants with varied technical backgrounds. Our focus group participants were divided into lay (FG0, FG2) and expert groups (FG1, FG3). Table 2 shows participants numbered in each group and their expertise. During the recruitment process, we sampled lay participants who had no knowledge of cryptography. As for the experts, we sampled participants who had knowledge of cryptography but no knowledge of functional encryption specifically.

Table 2. Participants in each focus group and their expertise.

Focus group number	Expertise	Participants
G0	Lay	P1, P2, P3
G1	Expert	P4, P5, P6
G2	Lay	P7, P8, P9, P10
G3	Expert	P11, P12, P13

The individual walkthroughs of the mock-ups had a focus on the UIs for the PIA and privacy by design descriptions as well as the risk reduction illustration (as seen in Figs. 2 and 3.

The focus groups included a group discussion of participants' inputs of the walkthroughs as well as investigating participants' perspectives and thoughts about (1) the presentation of the risks (2) understanding of the illustration and (3) thoughts on what is missing. The moderator facilitated the discussion by allowing each participant to first respond and then go around for comments.

Data from the focus groups were collected via the recordings, transcribed, and then coded via Nvivo (a qualitative data analysis software). The analysis of the data followed an inductive approach and we present our findings in Sect. 4.

3.2 Ethical Considerations

We submitted the proposal and study materials (including information letters, consent forms, and study guides) to the local ethical committee at Karlstad University and have received approval from the ethical advisor. Participation in the studies, the recording of the sessions, screen sharing, as well as the demographic questions were optional and based on the users' consent that we obtained before the studies. We provided an information letter about the studies, and consent forms with details about our data collection and processing.

4 Results: Walkthroughs and Focus Groups

Most participants clicked either on consent (6) or back (2) without going through the links in the first UI (Fig. 2a). The remaining five participants clicked through the UIs and reached the risk reduction visualization such as the ones found in

Fig. 3. The following results are based on the discussions of the focus groups mainly, as they indicate their input on the visualization of the risks as well as the PIA information provided.

Overall, all the non-experts except one in FG3 found the graph confusing and difficult to comprehend to some extent. Similarly, half of the experts (P4, P12, P6) specifically indicated that the graph was confusing and not understandable. Despite not directly mentioning confusion, the other half expressed several concerns about missing information and what they needed to know. In general, the confusion and difficulty in understanding the graph and our participants' concerns stem from different factors. There are issues with visual-related aspects, a diversion from what users expect of a typical graph, and more importantly insufficient information and clarification regarding the terminology used, the context, and the purpose. In the following subsections, we provide details about the sources of confusion, concerns, and difficulties participants experienced in understanding the PIA representation, along with what they appreciated.

4.1 UI Design Aspects

The use of different colors in the risk heat map (as seen in Fig. 3) to convey different levels of seriousness and likelihood was not appreciated equally and did not appear as intuitive for all of the participants. P11 found the'colorfulness' good because the colors "point to like negligible on the risk seriousness and likelihood". P8 made a connection with traffic lights and stated: "I think it is clear because of traffic lights, red is like no don't do that it's just dangerous, danger color, and green is like good, go, and yellow is in between". On the other hand, P9 found the colors confusing stating: "Why are there different colors ...? I don't know, and what does the mixture between different color, what does that mean? No idea". P9 requested clarification about what the colors and the arrows represent. Although no participants from non-experts voiced a comment regarding their appreciation of the graph, a few experts (3) commented on the validity of the graph and the fact that it was 'nice' in their opinion. P11 stated that "this depiction is like the standard like risk analysis results that you just put on this, like, graphical shape with different colors [..] But as a general graphical, like, a depiction it is valid". P5, similar to P13 who found the visualization 'nice' and 'ok', stated that "it could have been nice to keep the image". Despite positive opinions about the existence of such graphical representations among experts, P4 indicated uncertainty regarding the need for the visualization as they did not appreciate it: "I don't know to be honest. I don't want to say that I don't think there should be a like visualization, but yeah, I just don't know to be honest. But I did not like what I saw here anyway in front of me, yeah". P4 added that understanding such a graph requires a previous background in reading graphs: "If you're not used to looking at graphs this graph is probably confusing as well".

4.2 Deviation from Users' Expectations of a Typical Graph

Both P3 and P1 requested a graph that reads from left to right, contrary to the UI mock-up, as that is the way they are used to seeing and reading graphs. P3 stated that: "If I write a graph I have to start- yeah. From the left side to the right... I think the graph looks like it's upside down for me. Because the graph that I normally read starts from the left to the right. So, what I see here is a bit confusing. It's like...somehow the linear has to start from the left side and finish". P1 states: "It's not in the way I'm used- that I am used to when it comes to reading graphs and such...[] well... flip the graph. Somehow you need to move the axis to the right position as well, but just... the graph needs to start from the left and then go to the right. Yeah, that would help me at least". Despite the confusion, P1 believed that the context and the accompanying text helped clarify the graph better.

Experts as well as non-experts had specific expectations regarding the graph based on what they had previously seen. P6 expected to have scatter points and stated: "If it were like linear instead of just a grid. Because I understand that there are two variables, the seriousness and likelihood, but I... I don't know I would expect maybe scatter points".

4.3 Need for More Information and Clarifications

Non-expert participants' feedback generally included that they perceived the graph and text below it as reducing the risk. They believed the accompanying information made it clearer what the graph related to. For example, P1 conveyed that: "[..] seeing the graph confused me from the start, but when I read the text under, I can understand what you mean". Nevertheless, due to the lack of information about how the risk reduction would be accomplished and the similarity between the graphs showing two different types of risks, non-expert participants were confused about the purpose of the graph and what it really depicted, as P10 stated: "I don't see the purpose of this graph. Because it can be applicable for all kinds of risk and we don't see how it is reduced, so. It's just a graph saying you can have some big risks and you- We are trying to reduce them. But how do you try to reduce them? You have no idea". P7 also referred to the similarity of the graphs for different risks and said:"It is extra confusing that the same figure shows up here. I think it's the same. Risk likelihood, risk seriousness, yeah. Okay yeah, so that's confusing. [..] There is a missing description here. And I think a lot of this is incomplete". Despite understanding what the graph represents, P8 thought the purpose and credibility of the graph are unclear, as the graph and accompanying text do not convey how risk is reduced: "So, you know, it shows that they are simply making in such a way that the risk is neg- You can neglect it and also the likelihood is also decreased. So, I can understand what it says, but I can draw it myself. So, why is it there? I would like to know how are you doing this?".

In addition to the lack of information about risk reduction, non-expert participants also felt that the content provided was lacking in other aspects. Among these were the meanings of the two axes on the graph, risk seriousness and likelihood, the scales associated with them, and how risk seriousness and likelihood would correlate. For example, P7 stated: “I am uncertain what it shows. It does not show how they correlate. It says that the likelihood is reduced and the risks are reduced”. P9 also voiced their desire for more information about the labels included by adding: “I feel like there is too little information about what it means. This ‘Maximum’, ‘Important”’.

In a similar fashion to non-experts, experts wanted to know how risks were reduced, not just that they had been reduced. P11 stated that:“the only thing that is missing is that like why was that at that level and what controls were used to reduce it. Yeah, like so why was there before and what was done to move it there”. In addition, P5 wanted to know how the risks are mitigated with examples of risk evaluation: “but I’d need some risk that you really evaluated. [..] but just taking one or two examples and then on the image [..] showing that there, I don’t know from red color, for example, and then going into details to explain why you can take them to the green case”. Interestingly, experts disagreed regarding the usefulness of a graph lacking information about how risks are reduced. While P11 appreciated the graph by stating: “nice to see that this was the initial state, and this is the end state after the controls are applied”, P11 highlights: “it does not say how it has been done”. P4 and P5 did not like the graph/explanation and believed that it was not conveying much information as P5 said: “I don’t really like this explanation because it feels like you want to say something, but you don’t say enough to actually say something”. While familiarity with PIA and related backgrounds may have contributed to a positive opinion about the graph despite its lack of information (as mentioned by P11), it may not necessarily be a factor influencing users’ desire to know ‘how’ and not ‘what’.

In addition to how risks were reduced, experts wanted a deeper explanation of the exact meaning of the risks (e.g., illegitimate data access). Moreover, similar to non-experts, they wanted more clarity about the meaning of the risk seriousness and likelihood, and the meaning of the scales presented, as P13 stated: “Example of risk seriousness, what is high? [..] Some scale to- so that we can... more understand more easily... What risks means, and the likelihood what it means also”. The scales also appeared confusing for participants, as P6 mentioned: “the two-dimensional stuff doesn’t really give something better than just- probably just one dimensional... like very risky- like, what is it... like ‘Important’ to ‘Negligible’ or the other way around and just doing it one way. it’s too confusing.”

Participants in both groups, during the walkthrough, had the chance to see some information regarding the remaining risks which was conveyed below the PA graph as accompanying text (see Fig. 3b). Although very few (one expert and one non-expert) commented on the information regarding the remaining risks, it appeared that communication of such risks was appreciated as it could give users more information on what could happen to them and “that zone zero does not exist”, as P5 stated it. Still, P5 wanted to know more details about how personal data could be inferred or recovered from statistics.

5 Discussions

Based on our results, participants (lay and experts) have indicated their appreciation for the transparency of having information about privacy risk reductions. Therefore we believe providing information about risk reductions from the PIA tool to users is necessary. However, further clarifications and development of the visual aspects of PIA risk representations should take place. We present our recommendations for future work on usable PIA visualization in the following subsections.

5.1 UI Design Conventions and Clarifications

Participants showed varied opinions about the visualizations of the risks in terms of colors. The use of colors to illustrate the severity of risks could be considered useful in illustrating the seriousness of risks. In general, expert participants that were already more familiar with risk heat maps were more appreciative of the color scheme. However, due to the other information illustrated in the graph (arrows and simplified information), the perception of the color could have been affected accordingly. We, therefore, recommend design considerations when following conventions for the choice of color that must suit the target users, whether it is the familiarity with severity ratings (as used commonly in risk heat maps) or the accessibility for perceiving the colors presented correctly. Furthermore, a clarification for all UI elements must be available to users in a user-friendly manner.

5.2 Mental Models Considerations

As some participants were familiar with risk analysis and graphs in general, that created some confusion due to the mismatch in the mental models of some participants. Specifically, the arrow in the UI represents the transition of the risk from a higher risk seriousness/likelihood (up/right-hand side indicated by red) to a lower risk seriousness/likelihood (down/left-hand side indicated by green. This form of illustration (graph) has left participants, who are familiar with other types of graphs, confused. Their reasoning was that points should move from left to right and not the other way around. This format, which we used in the UI design, is taken directly from the PAPAYA tool, and participants who are familiar with risk heat maps seem to appreciate this format.

Furthermore, representing similar risk reductions for different risks seems to confuse participants. For example, the illegitimate data access and identification risks look the same in the UI as shown in Fig. 3. This could have had an impact on how users perceived the graph, as an image rather than a specific illustration of the risk at hand. Only those familiar with different risk types were able to notice the distinction. We, therefore, advise a consideration for the mental models and design conventions based on the target users, i.e., use risk heat maps with caution and possibly offer alternative illustrations for different users.

5.3 Need for More Information and Clarification Regarding the Terminology Used, the Context, and the Purpose

Participants indicated on many levels the need for more information and clarification regarding the terminology used, the context, and the purpose of the UI mock-ups. We, therefore, recommend improving the information provided on the following:

– Informing on the 'how', relating to how are the risks being reduced using the PETs. Providing information on 'how' the PET is done contributes to users' trust in the system. A graph like the one depicted in Fig. 3 was perceived by participants as a broad claim about risk reduction that anyone can make because it lacks the reasoning about 'why' the reduction is claimed in the figure. It should be made clear that the graph is based on a professional PIA tool, such as the one we used in PAPAYA.
– Clarifying the terminology used. Not all users, even experts, are familiar with the concepts of seriousness and likelihood in the context of risk management and it is better to exemplify them. Even the risks themselves (e.g. the meaning of illegitimate data access) should be clarified. Not knowing what the risk is makes it useless to know if and how it is being reduced.
– Taking precautions regarding remaining risks. To prevent PIA visualization from functioning as a privacy theatre (Privacy theatre dictates that PETs may provide the "feeling of improved privacy while doing little or nothing to actually improve privacy" [17]), we should always refer to remaining risks. By just emphasizing a lot on risk reduction, the remaining consequences of sharing data with a particular service and what it means for users to share their data are thwarted which can affect their decisions and may lead to regrets about sharing. The information about the remaining risks provided was also appreciated by the participants who got exposed to it. Therefore we recommend development of descriptions of remaining risks as seen in Table 1.

6 Conclusions

In our work, we show how PIA visualization in the user interface faces some challenges as well as opportunities for making the privacy-enhancing functionality and value of PETs transparent. Based on experts' and lay users' feedback, we present recommendations for future work and the development of usable PIAs for the transparency of privacy risks that should target different types of users.

Acknowledgment. We would like to acknowledge the PAPAYA (H2020 the European Commission, Grant Agreement No. 786767) and the TRUEdig (Swedish Knowledge Foundation) projects for funding this work. We extend our thanks to the project members for contributing with their valuable inputs throughout the projects. We further thank Tobias Pulls and Jonathan Magnusson for their technical input of the PAPAYA tool, John Sören Pettersson for his input to the user studies, and Elin Nilsson for her help in implementing the mock ups in adobe and transcribing results.

References

1. Privacy impact assessment (pia)—cnil. https://www.cnil.fr/en/privacy-impact-assessment-pia. Accessed 23 Jan 2023
2. Alaqra, A.S., Fischer-Hübner, S., Framner, E.: Enhancing privacy controls for patients via a selective authentic electronic health record exchange service: qualitative study of perspectives by medical professionals and patients. J. Med. Internet Res. **20**(12), e10954 (2018).
3. Alaqra, A.S., Kane, B., Fischer-Hübner, S.: Machine learning-based analysis of encrypted medical data in the cloud: qualitative study of expert stakeholders' perspectives. JMIR Hum. Factors **8**(3), e21810 (2021).
4. Boneh, D., Sahai, A., Waters, B.: Functional encryption: definitions and challenges. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 253–273. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19571-6_16
5. Bozdemir, B., et al.: D3.3 complete specification and implementation of privacy preserving data analytics—Papaya (2020). https://www.papaya-project.eu/node/157
6. Bozdemir, B., et al.: D4.3 final report on platform implementation and PETs integration—Papaya (2021). https://www.papaya-project.eu/node/161
7. Camenisch, J., et al.: Trust in prime. In: Proceedings of the Fifth IEEE International Symposium on Signal Processing and Information Technology, 2005, pp. 552–559. IEEE (2005)
8. Cavoukian, A.: Privacy by design, take the challenge (2009)
9. Cavoukian, A.: Privacy by design in law, policy and practice (2011)
10. Clarke, R.: Privacy impact assessments. Xamax Consultancy Pty Ltd. (1998)
11. Clarke, R.: Privacy impact assessment: its origins and development. Comput. Law Secur. Rev. **25**(2), 123–135 (2009).
12. Demjaha, A., Spring, J.M., Becker, I., Parkin, S., Sasse, M.A.: Metaphors considered harmful? an exploratory study of the effectiveness of functional metaphors for end-to-end encryption. In: Proceedings of the USEC, vol. 2018. Internet Society (2018)
13. EU-GDPR: Article 35 EU general data protection regulation. Data protection impact assessment. (2022). https://gdpr-info.eu/art-35-gdpr/
14. Simone, F.-H., et al.: D3.4 transparent privacy preserving data analytics (2021). https://www.papaya-project.eu
15. Heurix, J., Zimmermann, P., Neubauer, T., Fenz, S.: A taxonomy for privacy enhancing technologies. Comput. Secur. **53**, 1–17 (2015).
16. Karegar, F., Alaqra, A.S., Fischer-Hübner, S.: Exploring {User-Suitable} metaphors for differentially private data analyses. In: Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022), pp. 175–193 (2022)
17. Khare, R.: Privacy theater: why social networks only pretend to protect you (2022). https://techcrunch.com/2009/12/27/privacy-theater/
18. Murmann, P., Fischer-Hübner, S.: Tools for achieving usable ex post transparency: a survey. IEEE Access **5**, 22965–22991 (2017).
19. Nanayakkara, P., Bater, J., He, X., Hullman, J., Rogers, J.: Visualizing privacy-utility trade-offs in differentially private data releases. Proc. Priv. Enhancing Technol. **2022**(2), 601–618 (2022).