Context, Content, Consent – How to Design User-Centered Privacy Explanations

Wasja Brunotte*†, Jakob Droste*, Kurt Schneider*†
*Leibniz University Hannover, Software Engineering Group, Hannover, Germany
†Leibniz University Hannover, Cluster of Excellence PhoenixD, Hannover, Germany
Email: {wasja.brunotte, jakob.droste, kurt.schneider}@inf.uni-hannover.de

***Abstract*—In the context of the ongoing digitalization of society, human values such as privacy, ethics and trust are becoming increasingly important. Digital systems are entering private and professional spaces, which in turn affects the privacy of their end users. Hence, there is a need for conveying privacy information in a transparent and understandable manner, with the user in the focus. Lawmakers introduced privacy policies as a means of communicating privacy information. However, those documents have proven to be practically useless for end users. Privacy policies are long, vague, ambiguous and use complex language, such as legal terms, which often require profound background knowledge. Explainability has shown potential as a means to increase transparency and foster trust in software systems. Based upon the foundation of explainability, we developed a layered concept for user-centered privacy explanations, which is implemented within a high-fidelity software prototype. Finally, we tested and evaluated our concept by conducting an interactive user study with 61 participants. The results of our study suggest that our layered design concept enabled participants to understand the privacy aspects they regarded as important. We conclude that our approach seems to be an appropriate way to communicate complex privacy information to end users.**

***Index Terms*—Privacy, Privacy Explanations, Explainability**

I. Introduction

Software systems accompany and support us in our everyday lives, e.g., at work, when consuming information, when purchasing or distributing goods, and when keeping in touch with friends. Human values such as accessibility, ethics, privacy, transparency, and trust are playing an increasingly important role for software engineers [1]. Due to the great advantages that digital systems offer us, users tend to forget that they are not just consuming information. Users reveal a lot of private information about themselves when interacting with digital systems. Often this happens without explicit knowledge and consent of the users [2], [3].

In an effort to protect end users and their online privacy, the European Union has introduced the General Data Protection Regulation (GDPR) in 2018. Article 12 of the regulation [4] states that the processing of personal data must be explained "in a concise, transparent, intelligible and easily accessible form, using clear and plain language". However, this is at odds with the form in which privacy information is usually encountered in today's digital spaces. On the one hand, we have privacy policies that are long, unreadable and purposefully opaque [2], [5]. On the other hand, there are short form privacy notices such as cookie banners, which are unspecific, unclear and were found to employ dark design patterns, aiming to confuse end users [6].

Software providers are legally and morally obligated to provide end users with accessible and suitable explanations on how their personal data is processed. However, they do not have the means to achieve this at the current point in time. Hence, there is a need for ways to convey privacy information in a form that is both understandable and satisfying for end users. To bridge this gap in research, we propose *privacy explanations* since they may have the potential to remedy this problem. Furthermore, Brunotte et al. [3], [7] have shown that they can foster end users' trust in software systems. This could also be an incentive for commercial software providers to employ privacy explanations, as an increased end-user trust might be in their corporate interest and might lead to more customer loyalty as well as a positive company image [3].

Within this work, we build upon our previous research [3] and investigate privacy explanations through the lens of explainability. The goal of this work was to investigate how to design user-centered privacy explanations that meet the needs and expectations of end users. To this end, we adapt two types of explanations from the field of explainable artificial intelligence (XAI) - *contrastive explanations* and *example-based explanations* - and embed them within a layered structure for privacy explanations. We evaluate our design within an interactive user study with 61 participants, which includes the navigation of a prototypical implementation of those concepts. Our results suggest that our design is able to effectively and appropriately convey privacy information to end users. Furthermore, they support the notion that privacy explanations have a positive influence on end user's trust in the software system as well as on their privacy awareness and underline the importance of context, content, and consent.

II. Background and Related Work

Online privacy "is about an individual's control over their personal information in virtual space and their right to withhold this information" [3]. Individuals should have the right to know by whom their data may be accessed and also at what point in time this occurs. It is precisely this gap that privacy explanations address. The current state of the art and, thus, the primary channel to inform users about the data practices of a service provider, are documents such as privacy policies or short privacy notices. However, these kind of documents are insufficient to inform users with respect to their privacy. They are too long, too vague, and too hard to understand [2], [5]. As a result, these documents are often ignored by end users. Privacy explanations can be an alternative to educate the user in a transparent and comprehensible way. In light of this, a privacy explanation is not a document such as a privacy notice, privacy statement, or privacy policy. Instead, it is literally an explanation regarding a certain privacy aspect. This means that a privacy explanation is "a piece" of information that is given by a system in a specific context to an addressee (e.g., end users), with the aim of informing and educating the addressee about a specific privacy aspect. Due to space limitations, we refer the reader to [3] for our formal definition.

III. Research Goal and Design

The goal of this work was to investigate how to design user-centered privacy explanations that meet the needs and expectations of end users. Data from a previously conducted survey [3] formed the

DOI reference number: 10.18293/SEKE2023-032

basis, which we validated and extended through a literature review (LR) in the area of explainability and privacy.

By means of the gathered data, we conceptualized and refined our vision of user-centered privacy explanations and developed a high-fidelity prototype, which we evaluated through an interactive user study. The focus of this paper is on the results obtained through the qualitative research we conducted. Due to space limitations, we refer to our supplementary material for more details on our approach, especially the conduction of the LR, validation process as well as the user study [8]. Our research was framed by the following research questions (RQs):

> **RQ1:** What relevant information should a privacy explanation contain to meet the needs of end users?
> **RQ2:** What are appropriate strategies for designing user-centered privacy explanations to convey the relevant information?

RQ1 focuses on investigating what information is required to inform and educate end users. Here, it is important to consider the *relevant information* that, on the one hand, fits into the context of current data use (scope), and on the other hand, meets the expectations and needs of the users. One challenge is to present satisfactory information without confronting the user with long texts, similar to a privacy policy. By the means of **RQ2**, we want to assess how to design user-centered privacy explanations. We need to investigate implementation strategies of how to incorporate privacy explanations into a system. Therefore, it is necessary to translate the high-level requirements into concrete design choices.

A. Research Design

1) Literature Review - Validation of Survey Data: In our previous work [3], we conducted an online survey to identify the need for privacy explanations. The data resulting from this survey forms the foundation of our concepts. The data revealed that, in addition to privacy, the NFRs transparency, understandability, trust, and trustworthiness in particular stood out as critical for privacy explanations. For this work, we supplemented the previously conducted survey with a thorough LR in the area of explainability and privacy, with respect to the aforementioned NFRs. The aim of this step was to validate the data we obtained against literature and to broaden our knowledge.

The starting set for our LR originates from an LR in the field of explainability by Chazette et al. [9]. Our work extends this LR by conducting additional steps of snowballing as well as a data base search. Both with a focus on the relationship between privacy and explainability. We scanned the final set from Chazette's SLR for relevance concerning the NFRs explainability, privacy, transparency, trust, trustworthiness as well as understandability, and conducted our snowballing process in accordance with Wohlin's guidelines [10].

2) Conceptualizaton & Prototyping: We approach our concepts for user-centered privacy explanation in two steps. First, we collated and analyzed our data from the previous step in order gain a deeper understanding of what are relevant information and privacy aspects for providing satisfactory and understandable privacy explanations. Here, we identified the importance of context, content, and consent to which we continue to refer to as the *3C-principle*. Second, we conceptualized these findings within our design for privacy explanations and incorporated them into the conception of the high-fidelity prototype.

3) User Study Design: To evaluate our concept, we conducted an interactive user study with 61 participants. We invited our personal networks to participate in and share our study. Subsequently, we made appointments with those who replied positively. The study consisted of three main sections. It was provided in the form of an online survey, which included two questionnaires and an interactive section in the middle, which made use of a high-fidelity privacy explanation prototype. The prototype was designed in accordance with our previously described concepts. All participants were asked to use the "Think-Aloud" approach throughout the whole study. While completing the questionnaire and interacting with the prototype, they were encouraged to comment and reason their decisions. The results of the coding process of participants remarks can be found in our supplementary material [8].

IV. Relevant Information for Privacy Explanations

Requirements for Privacy Explanation. As end users come with all kinds of different knowledge and backgrounds, they have different needs and attitudes when it comes to privacy. In order to provide meaningful privacy explanations, we must first understand what privacy aspects are required to be explained. Privacy explanations essentially pursue two abstract quality goals: *what information is legally required* and *what information is required by users*. From these superordinate goals, further requirements can then be refined. We were able to elicit a set of high-level requirements in our previous work [3], which we confirmed through our LR. We found evidence in the literature that the four clusters of the requirements are justified: Data Usage, Data Storage, Confidentiality, and Presentation. The cluster **Data Usage** educates a user *what*, *why*, and *how* data is collected [11]. We summarize these two W-questions and one H-question as the **2W1H** principle. It was also found that users attached importance to the question *"what happens in case of non-consent?"*. **Data Storage** comprises information about where and how long the data is stored [4]. Information about the deletion, and if safeguards are taken into account, is also included in this cluster [3]. Safeguards refer to precautionary measures such as encrypted storage of data, access restrictions, etc. **Confidentiality** provides information on, among other things, who has access to the data and whether the data is resold [11]. The **Presentation Form** determines what a privacy explanation should look like, both on a linguistic level and in terms of the medium (textual, visual, audio) [9].

Context, Content, Consent – 3C-Principle. The analysis of the literature revealed that privacy explanations can essentially be embedded in three key points: context, content, and informed consent (3C-principle). In general, context is characterized by a specific situation involving a person, a system, a task, and an environment [9]. In the case of privacy explanations, we speak of context when a system processes, requests, or obtains explicit or implicit permissions (e.g., a smartphone app needs access to the camera) to perform a specific task. With reference to our definition, a privacy explanation is always context dependent (contextual) [2], [12]. Thus, a system should contextually supply its user with the needed information – the privacy explanation.

The content is aligned with the context and thus relates directly to it. Content plays an essential role in terms of the effectiveness of the information presented and is framed by the design and structure of the presented explanation (presentation form). This implies that the content is also shaped by the needs of the respective end users. With respect to privacy explanations, the content covers the requirements cluster data usage, data storage, and confidentiality.

When, in a given context, a privacy explanation is presented to the user, it is done with the aim of informing and educating users about the use of personal data in the given situation. This should enable them to make an *informed consent* about the use of their personal information [5]. A privacy explanation should not make use of so-called dark patterns such as *forced consent*, as that would be in complete contrast to the actual purpose.

Answering RQ1: End users want to be informed about privacy matters in accordance with the 2W1H principle. They also expect to learn whether they will face any disadvantages if they do not consent to data use. Information about the storage of data is also considered relevant. Providing users with this relevant information, according to the current context, puts them in the position to give informed consent, respects their right to self-determination, and might even foster their privacy awareness.

V. Designing User-centered Privacy Explanations

In the following section, we will build upon our findings concerning RQ1 to propose appropriate strategies for designing user-centered privacy explanations. Furthermore, we answer RQ2 by discussing the results of our user study, in which our concept was evaluated.

Conceptualization - A layered Approach. In order to effectively inform end users, we need to provide them with an explanation complexity that fits their background knowledge and needs. In this context, previous works have argued for the potential of personalized [13] or layered explanations [3], [5]. For our **presentation form**, we chose to provide privacy explanations in a layered manner. Note that the layers do not build upon each other. Instead, each layer contains its own set of privacy aspects. This way, all necessary privacy information is readily available and accessible, and users can decide for themselves which parts they want to read, without being overloaded with information. Using our defined requirements for privacy explanations as a basis, we introduce five layers of privacy explanations. Each layer covers different privacy aspects, and altogether, they include all necessary privacy information.

The first two layers of the privacy explanation are focused on **data usage**, using regular text explanations and contrast. Within the first layer and in accordance with the 2W1H principle, end users are told what data is used, why it is used and what happens in case of non-consent. This baseline explanation is critical for end users' understanding of how their data would be used and enables them to decide, whether or not to consent to that processing. The second layer of the privacy explanation is a contrastive explanation, which, as the name implies, stands in contrast to the baseline explanation. Contemporary explainability research has found contrastive explanations to be an effective way to convey information to end users [12]. Within the contrastive layer of the privacy explanation, we tell users in which ways their data will not be used, if they choose to permit processing.

A proven **presentation form** that can provide additional context to end users are example-based explanations. Adadi and Berrada [12] state that "amongst agnostic methods, visualization is the most human-centered technique". Within the third layer of our privacy explanation, we opt to provide example-based explanations. Ambiguous explanations about how data is being processed can lead to decision that do not suit end users' actual privacy preferences [14]. Providing a visual example should be an efficient way to solve this issue. Furthermore, by choosing examples that fit the software system and its typical use cases (contextual), we can provide additional context for the end user. Within the forth and fifth layers, we provide information on additional privacy aspects for interested end users. In essence, these layers are covering details on **data storage** and **confidentiality**, as described in our previously defined requirements for privacy explanations. The forth layer explains the circumstances of **data storage** and the rights of the end users. The fifth and final layer consist of a third party explanation, which lists all third parties who would gain access to the data and briefly states how they might process it [4].

Results from the Study. When comparing the different types of explanations with each other, we employed the *Wilcoxon Signed-Rank* test to test for statistical significance. With the exception of the example-based explanation, most participants (85%) perceived all layers of the privacy explanation to be relevant to their needs. In particular, participants evaluated the example-based explanation as less relevant than the baseline explanation (statistically significant with $z = 4.16404$, $p < 0.00001$). While every other explanation layer was seen as important on average, the examples were only moderately important to the average participant. While "thinking aloud", 15% of participants commented that they thought the examples were not necessary, as they added no new information, but only provided another presentation form for privacy aspects that were already explained. In the vast majority of cases, participants had no problem understanding the privacy explanations.
In their "Think-Aloud" comments, 26% of participants attributed this to the explanations being short and concise. 39% highlighted a positive effect of the layered approach on the explanations' understandability. Both the contrastive and the example-based explanations have shown to be suitable forms of privacy explanations, when it comes to their understandability. In particular, the example-based explanation was regarded as more understandable than the baseline explanation (statistically significant with $z = -2.53252$, $p < 0.01$). Furthermore, 43% of participants specifically commented on the importance of providing helpful examples. 30% of participants highlighted the importance of the contrastive explanation, remarking that it addressed some of their pre-existing privacy worries.

Answering RQ2: Concerning the design for privacy explanations, we find that successful strategies comprise proper explanation types, using suitable presentation forms, within a layered structure. Both, the contrastive and example-based explanations have shown to be understandable and relevant to our participants. Privacy explanations should stay short and concise. This can be supported by the use of visual examples. The layered approach was successful in providing our participants with privacy information in a manner that suits their needs. The vast majority of participants found the explanations to be understandable. We attribute this to our layered approach, that broke up the large amount of information and provided structure to it.

VI. Discussion and Threats to Validity

The first contribution of this work is a comprehensive overview of relevant information that should be included in a privacy explanation. This information frames the needs an expectations of end users regarding their privacy and is aligned with our identified 3C-principle, which shapes our design concept for user-centered privacy explanations. Context in which privacy explanations are given, as well as their timing, are of crucial importance [9] and already embedded in their definition [3]. Making use of examples is a prime opportunity to provide context, as they can show how a specific application would process data in a common usage scenario. Notably, the results of our study have shown a discrepancy between example-based explanation's perceived importance and understandability. Even though the information provided via the examples was seen as the least important, it was perceived as significantly more understandable to participants than the textual explanations. In accordance with [12], we conclude that using visual examples, and thus providing context, is indeed an effective way to explain privacy information to end users. However, the examples need to be carefully chosen and should not include redundant information if possible. According to the GDPR and backed by the findings of our LR, the contents of privacy explanations should mainly be characterized by answers to the 2W1H questions, and should be enriched with non-consent information as well as information on the storage and retention of private user data. Information about who has access to their data and whether it is aggregated or resold might also be considered important by end users. It is important to note here that not all information is equally relevant for every user, as different users have different privacy attitudes [3].

Our second contribution are our strategies for designing for user-centered privacy explanations. The results of our study suggests that the layered approach is a suitable solution to the issue, as it addresses the challenge of providing appropriate information granularity for the different needs of end users. Doing so, we can meet the different needs, expectations, and attitudes of different end users. We refer to this as achieving *informational completeness*. Following this line of thought, we call our concept *user-centered inclusive design*, since it does not exclude any user and takes into account their respective privacy attitudes. The results of our research on privacy explanations suggest that they contribute to better understanding, inform and empower users. Thus, privacy explanations can lead to informed consent by the end user, which in turn has a positive impact on their privacy awareness, because users are sensitized through education. In light of this, genuine informed consent is only possible if both context and content are appropriately supplied [15], and this is exactly the approach we would like to address with our proposed user-centered inclusive design.

A. Threats to Validity

Despite careful planning and execution of our research approach, there are still some threats to validity regarding our obtained results. **Literature Review**. The review process requires a common understanding of the methods and concepts used by all researchers. Results could be subject to bias if methods and concepts are misunderstood. We mitigated this threat by establishing and discussing a review protocol to achieve a sufficient common understanding. We formulated inclusion and exclusion criteria to reduce bias due to subjective decisions in our selection process and conducted the data analysis independently. When opinions differed, the results were discussed until consensus was reached among the researchers. **User Study**. Although 61 participants provide a substantial sample size, some of the conclusions might be affected by it and should not be overgeneralized. Our strategy to select the participants has some limitations and might not reflect the whole population which may threaten the global generalizability of our results. The majority of our participants had profound information technology (IT) knowledge, i.e., this fact may not consider people who have difficulties operating software systems. However, we did not find any evidence of this threat impacting our results. Instead, we gained valuable insights into what different people think and what their attitudes are toward privacy. The perception and understandability of explanations is hard to measure. We handled this threat by using statistical tests where appropriate and using more qualitative analyses otherwise.

VII. Conclusion and Future Work

Privacy is one of the human values in software engineering and is becoming increasingly important in our highly interconnected world. In order to provide end users with their right to (online) privacy when using software systems, it is important to enter into a dialogue with them about a system's data practices. To this end, we researched a novel concept of user-centered privacy explanations, to educate end users regarding their privacy. Based on survey data and validated through an LR, we elicited high-level requirements for privacy explanations. We refined the requirements into context, content and consent (3C-principle) which shaped our design concept for user-centered privacy explanations. We evaluated our concept in a user study, by embedding it into a high-fidelity prototype. Our results suggest that our layered design concept, in line with the identified 3C-principle, enabled participants to understand the privacy aspects they regarded as important. In conclusion, we hold that our approach seems to be an appropriate way to communicate complex privacy information to end users and brighten their sensitivity with respect to their privacy awareness. As future work, we plan to integrate privacy explanations into an existing software system, as a next step to evaluate them in terms of suitability and usability.

Acknowledgments

This work was funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy within the Cluster of Excellence PhoenixD (EXC 2122, Project ID 390833453), and supported under Grant No.: 470146331, project softXplain (2022-2025).

References

[1] J. Whittle, M. A. Ferrario, W. Simm, and W. Hussain, "A Case for Human Values in Software Engineering," *IEEE Software*, vol. 38, no. 1, pp. 106–113, 2021.

[2] W. Brunotte, L. Chazette, L. Köhler, and K. Schneider, "What About My Privacy? Helping Users Understand Online Privacy Policies," in *Proceedings of the ICSSP'22*. New York, NY, USA: Association for Computing Machinery, 2022.

[3] W. Brunotte, A. Specht, L. Chazette, and K. Schneider, "Privacy Explanations –- A Means to End-User Trust," *Journal of Systems and Software*, vol. 195, p. 111545, 2023.

[4] European Parliament and Council, "General Data Protection Regulation," https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504, 2016, accessed: 16.07.2022.

[5] L. F. Cranor, "Necessary but not sufficient: Standardized mechanisms for privacy notice and choice," *J. on Telecomm. & High Tech. L.*, vol. 10, p. 273, 2012.

[6] M. Nouwens, I. Liccardi, M. Veale, D. Karger, and L. Kagal, "Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence," in *Proceedings of the CHI Conference*, 2020, pp. 1–13.

[7] W. Brunotte, L. Chazette, and K. Korte, "Can Explanations Support Privacy Awareness? A Research Roadmap," in *IEEE 29th RE Conference Workshops (REW)*, 2021, pp. 176–180.

[8] W. Brunotte and J. Droste, "Supplementary Material for Research Paper "Context, Content, Consent – How to Design User-Centered Privacy Explanations"," https://doi.org/10.5281/zenodo.7911904, 2023.

[9] L. Chazette, W. Brunotte, and T. Speith, "Exploring Explainability: A Definition, a Model, and a Knowledge Catalogue," in *IEEE 29th RE conference*. IEEE, 2021, pp. 197–208.

[10] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *Proceedings of the 18th EASE conference*, 2014, pp. 1–10.

[11] S. Pötzsch, "Privacy Awareness: A Means to Solve the Privacy Paradox?" in *The Future of Identity in the Information Society*, V. Matyáš, S. Fischer-Hübner, D. Cvrček, and P. Švenda, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 226–236.

[12] A. Adadi and M. Berrada, "Peeking inside the black-box: a survey on explainable artificial intelligence (XAI)," *IEEE access*, vol. 6, pp. 52 138–52 160, 2018.

[13] K. Sokol and P. Flach, "One explanation does not fit all," *KI-Künstliche Intelligenz*, vol. 34, no. 2, pp. 235–250, 2020.

[14] H. Fu and J. Lindqvist, "General area or approximate location? How people understand location permissions," in *Proceedings of the 13th Workshop on Privacy in the Electronic Society*, 2014, pp. 117–120.

[15] A. E. Waldman, "Privacy, Notice, and Design," *Stanford Technology Law Review*, vol. 21, p. 74, 2018.