Structural and functional explanations for informing lay and expert users: the case of functional encryption

Ala Sarah Alaqra
Karlstad University
as.alaqra@kau.se

Farzaneh Karegar
Karlstad University
farzaneh.karegar@kau.se

Simone Fischer-Hübner
Karlstad University &
Chalmers University of Technology
simone.fischer-huebner@kau.se

ABSTRACT

Usable explanations of privacy-enhancing technologies (PETs) help users make more informed privacy decisions, but the explanations of PETs are generally geared toward individuals with more technical knowledge. To explain functional encryption (FE) to experts and laypersons, we investigate structural and functional explanations and explore users' interests and preferences, as well as how they affect users' comprehension and decisions about sharing data. To this end (with an EU-based population), we conducted four focus groups, in combination with walk-throughs, with 13 participants in the first study, followed by an online survey with 347 experts and 370 laypersons. Both explanations were considered useful in fulfilling the different needs of participants interested in the privacy policy information. Participants, regardless of their expertise, trusted and were more satisfied with the structural explanation. However, functional explanations had a higher contribution to all participants' comprehension. We, therefore, recommend combining both types of explanations for a usable privacy policy.

KEYWORDS

functional encryption, functional & structural explanation, transparency, privacy, usability, user comprehension, mental models

1 INTRODUCTION

The growing use of the internet exposes users to privacy and security threats on a constant basis. Studies show that insufficient user knowledge is a factor for users not taking actions of data protection measures [33]. User consent is a means to allow user control and provide transparency about the usage of user data, which is legally supported. The EU General Data Protection Regulation (GDPR) dictates that consent must be informed and unambiguous [17]. Following the support of legal efforts, Privacy Enhancing Technologies (PETs) aim to address privacy and security challenges in order to mitigate online threats to users' data. However, the process of informing users and providing usable explanations of PETs is a challenge. According to Recital 42, Article 7, of the GDPR: "For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended" [17]. The challenge of informing users extends with the fact that the design of security descriptions does not seem to be usable for end users [6].

Proceedings on Privacy Enhancing Technologies 2023(4), 359–380

https://doi.org/10.56553/popets-2023-0115

Our objective is to investigate usable explanations for a privacy-enhancing cryptographic scheme. The scheme is in the form of functional encryption (FE) [10], which has recently received attention as a potential enabler technology for implementing privacy-enhanced machine learning on encrypted data. FE is an encryption scheme, which enables data owners to authorize a third party to compute a specified function on encrypted data. While the data owners' data is kept confidential from the third party (through encryption), the computation results are in plain-text (i.e. in unencrypted form).

Explanations of the underlying technologies in a system, service, or product may cue the structural or functional mental models of users. Andrea diSessa [15] distinguishes structural from functional mental models in terms of their contextual specificity. Structural models contain information about the structure of, for example, a system and are independent of specific tasks. Functional models, on the other hand, are task-related and contain information about how to use a selected set of functions to perform a specific task. Therefore, explanations based on structural models (herein structural explanations) focus on providing details of how a system works, whereas explanations based on functional models (functional explanations) focus on certain properties of a system that are necessary to complete a task, i.e. what a system can do.

In the context of encryption, previous research, based on the results of studies conducted with non-experts, has noted that structural descriptions are likely to be less effective than functional descriptions when the aim is to improve users' understanding of a complex system [7, 14]. However, previous research reports that experts and non-experts have different goals, preferences, and requirements when using privacy and security systems [18, 28]. It suggests that experts and non-experts in the context of encryption may also have different requirements for the information they need for making decisions, opinions, and interests regarding the type of explanations. Therefore, as part of our research objective, we want to explore how technical knowledge of encryption may impact preferences and comprehension of the two forms of the explanations provided (functional and structural) for FE. The context of our research study is a privacy-preserving analytics use case, where mobile users are asked to give consent for their mobile usage data to be shared in functionally encrypted (and thus protected) form with a data analytics platform, which can then calculate specified statistical analytics functions on the data (see section 2.2). In this work we address the following research questions:

RQ1: What are lay and expert users' interests, opinions, and preferences of privacy information including FE explanations?

RQ2: What are the implications of the FE explanations on lay and expert users' decisions to share their data with a data analytics platform?

RQ3: What is the impact of structural and functional explanations of FE on lay and expert users' comprehension?

Providing usable explanations for a PET as part of privacy notices in consent forms, which are well understood and of interest to the users, are relevant for enabling informed decisions and taking control over personal data. Additionally, understanding the underlying privacy-enhancing mechanisms can, according to [20], also promote trust. However, explaining PETs still poses a special challenge. This is especially the case if PETs, such as FE and homomorphic encryption, are novel for users and different from traditional (encryption) schemes that the user may have heard of or are familiar with. Furthermore, they could be perceived as counter-intuitive, as no existing real-world analogies exist [5]. Therefore, research on usable explanations of FE (and of PETs in general), which can contribute to usable privacy notices as part of consent forms, requires further work.

For the purpose of our study, we consider experts as users with technical expertise in cryptography who however lack technical knowledge about FE, while laypersons, or non-experts, are 'lay' in terms of cryptography expertise. To address our objective and research questions stated in Section 1, we followed a mixed-method approach by conducting two user studies. In an exploratory sequential design, first, we conducted qualitative user studies consisting of user interface (UI) mock-ups walk-throughs and focus groups (study A). Participants of study A explored both explanations and results from study A led to forming of three hypotheses relating to differences in preferences and comprehension of functional and structural FE explanations between experts and non-experts. The second study (study B) was an online survey with targeted participants (experts and lay participants were screened in a pre-study). The survey's purpose was to test the hypotheses formed and provide a further investigation of our research questions and focused on the comprehension of the individual explanations. The survey mainly consisted of quantitative data collection and analysis.

2 BACKGROUND AND RELATED WORK

2.1 Functional encryption

Functional encryption is an encryption mechanism enabling a party, which has the functional decryption key (a.k.a. evaluation key), to learn an authorized function of the encrypted data [10]. The data owner, Alice, who holds a master secret key can provide another party, Bob, with the evaluation key, which is related to a function f and allows Bob to learn the result of f applied to Alice's data. Bob is then authorized to only execute the function, for which he has obtained the evaluation key, and nothing else. In contrast to homomorphic encryption, which produces results in the form of ciphertext, Bob gets the result of the computation in an unencrypted form. FE can be used for various use cases, which require analyzing confidential data in a privacy-preserving manner. Examples of FE use cases include spam filtering on functionally encrypted emails allowing to perform spam classification functions while keeping the email content confidential. Another use case can be privacy-preserving big data analytics. For instance, consider a use case where patients want to contribute their medical data for statistical research purposes without putting their privacy at risk. For protecting the patients' privacy, their data are sent to an analytics platform in functionally encrypted form. Medical researchers (with access to respective evaluation keys) can then perform statistical functions on the data. The next section presents the FE use case that we used for the context of our studies, which provides another example illustrating how functional encryption can be utilized as a basic building block for implementing privacy-preserving data analytics.

2.2 The use case scenario

Our work was performed as part of the evaluation of a privacy-preserving smartphone usage analytics use case developed in the PAPAYA EU project. In a slightly adapted scenario of this use case (presented in [13]) that we used for our evaluation, there are three types of main actors: users/individuals, a Telecom provider *TeleCom AB* and a third party *MediaSurvey*. Users interested in contributing to statistical surveys would first install an app provided by Telecom AB. A third party, such as *MediaSurvey*, is interested in obtaining insights on mobile usage data and can request from *TeleCom AB* to collect and analyze mobile usage data from users. Users would be asked to consent to participate in a statistical survey and to share their data for the purpose of this survey in a privacy-preserving manner. In our scenario, *MediaSurvey* sends requests to receive statistics from *TeleCom AB* on social media usage data related to the users' ages. The mobile apps, of the consenting users, collect and aggregate usage data (on social media usage, age), encrypt them, and send the encrypted aggregated data to *TeleCom AB*. *TeleCom AB* then performs statistical analytics on the encrypted data. The statistical survey results are then sent to *MediaSurvey*, which has requested the statistical survey and can obtain the statistical results in plain (unencrypted) form (see Figure 1).

The use of functional encryption ensures that the statistical analytics can be performed in a privacy-preserving manner on encrypted data so that the users' raw data (i.e., their social network usages, age) are not accessible in plain (unencrypted) form by *TeleCom AB* and by *MediaSurvey* who only learn the statistical results.

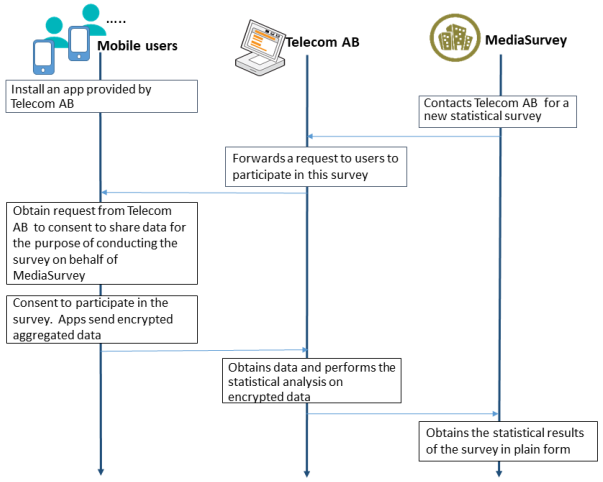


Figure 1: Use case scenario overview

2.3 Related work

2.3.1 Mental models of encryption. Based on the results of a qualitative study exploring user perceptions of encryption, Wu et al. [32] conclude that teaching how encryption works will not help users form correct mental models. Instead, they recommend aligning explanations with functional models that users already possess. For this reason, recent research exploring the users' understanding of end-to-end encryption (E2EE), focused on analyzing the comprehension of functional explanations and metaphors for E2EE communicating the benefits and limitations of E2EE to lay users and supporting them to construct functional mental models [1, 3, 14, 29]. Demjaha et al. [14] point out that encryption itself is a "technical cryptographic term", and consequently they derive and analyze metaphors for E2EE that are not based on the term encryption.

Based on an online user study [2], Akgul et al. however recently showed that explaining the provided security functionality of an E2EE tool as "encrypted communication" or "military-grade encrypted communication" (rather than as simply "secure communication" or with the more precise term "end-to-end encrypted communication") increased the study participants' perceptions that the tool was appropriate for privacy-sensitive tasks. They thus assessed "encrypted" to be a relatively well-understood term and to be the most useful security or privacy indicator for people.

Also, another recent study [16] investigating the effect of the wording of encryption on users' perceived security, reports that the technical terms "encrypt" and "secure" have outperformed lay wording "translating to secret code".

Bai et al. also observed in an exploratory study with lay users that technical details about E2EE that were presented in proposed tutorials were most effective when these explanations were functional [7]. While some study participants were interested to know how E2EE works, most did not find it important, and a strong risk of misunderstanding structural technical explanations was observed. Our study is the first, to our knowledge, that explores and compares the user's (experts and laypersons) understanding and perception of functional encryption when using functional versus and in combination with structural explanations.

2.3.2 Experts' vs laypersons' perception of privacy and security. Previous studies that compared laypersons' and experts' mental models of privacy tools observed commonalities and differences between their perceptions and understandings of privacy tools and the risks involved. Camp et al. [12] showed earlier that experts and non-experts have two different mental models for many security and privacy risks. Experts' deeper technical understanding of the underlying technical operations and threat models was observed by Gallagher et al. [18] in a study conducted with both experts and non-experts on their mental models of the Tor network. A recent study by Brinkhorst et al. [9] found that the mental models of VPNs (Virtual Private Networks) between experts and non-experts are in general similar. Nonetheless, while experts have a deeper technical understanding of VPN technology and of the involved threat models, they still sometimes hold false beliefs about the security aspects of VPNs. In a qualitative study involving both laypersons' and administrators' mental models of HTTPS, Krombholz et al. [22] showed that laypersons' mental models are more conceptual while administrators' mental models are rather protocol-based, frequently containing protocol components and technical terms but still may lack an accompanying understanding of their functionality. De Luca et al. [24] compared expert and non-expert attitudes toward (secure) Instant Messaging. Their study concludes that experts had 'technology-focused mental models'. Experts less trusted the term 'private' or 'secure' instant messenger because they perceived it as marketing and/or because they were aware of technical limitations for protecting the privacy and the impossibility of achieving 'perfect' protection. Seven of the 15 interviewed experts stated that they would check the technical details of the messenger, and six experts requested audits for verifying such claims, while in contrast, most interviewed non-experts stated that they would trust service providers to use such claims correctly or would decide based on recommendations by their tech-savvy and trusted peers. Other studies [4, 5, 23] show that also for other reasons technical experts may even have less trust in the claimed privacy functionality of privacy-enhancing crypto tools if they have functionalities differing from those of traditional crypto schemes that they are familiar with. Given these observed differences in mental models and the trust of technical experts and non-experts, our study aims to investigate whether technical background knowledge could be a factor. Specifically, we aim to investigate experts' and laypersons' interests and preferences of the structural and functional FE explanations and the effects of the explanations on different users' comprehension and decisions.

3 STUDY A: WALK-THROUGHS AND FGS

The first study (Study A) of our mixed-method approach consists of two parts, UI mock-up walk-throughs followed by focus group discussions, see Appendix A for the detailed protocol of the study. Both parts were conducted online via Zoom, due to the COVID-19 pandemic's restrictions at the time. Participants were individually interviewed for part one (UI mock-up walk-throughs) in parallel Zoom rooms, and after a short break, the focus groups commenced. The moderator of all focus groups is the main author, while co-authors who were not present viewed the recording afterwards. We sampled participants based on their technical backgrounds in cryptography and grouped them into lay and expert user groups in our study. We recruited participants using our network to find both users with a technical background in cryptography, but without the knowledge of functional encryption, and laypersons (non-experts in cryptography). Participants volunteered to participate in the study, and no compensation for participants was mentioned. In our pre-study correspondence, once recruits confirmed their interests, we sent out an email with an information letter and a copy of the consent form as well as scheduling details for the study to take place. We conducted four FGs with both experts and laypersons during March 2021 (on March 12th, 19th, 25th, and 30th of 2021) (see Section 3.4 for more details on participants). The duration of the focus groups was approximately 2 hours (30 minutes for consenting and introductions as well as walk-throughs, and 90 minutes for the focus group discussions). Data Saturation during each focus group was reached when no new comments were added after each phase of go-arounds. Due to the format of the study involving rich discussions, we had enough data already with the two FGs, however, we conducted additional FGs for both experts and laypersons for

more robust results. We reached data saturation with the third and fourth FGs (FG2, FG3), and the criteria of having the perspectives of both types of users, lay and experts were fulfilled.

Ethical considerations. The reported studies (A and B) in this paper have received the ethical approval of the local ethics advisor at Karlstad University. We processed data in compliance with the GDPR as well as the university's local policy. Consent was obtained prior to the beginning of all studies, including the prescreening study. Participants of study A were offered a gift voucher as a token of our thanks only after the completion of the focus groups in an effort to avoid biasing them with monetary incentives, as mentioned above. Participants of study B (prescreening study and the main survey) were paid according to the minimum hourly reward on Prolific at the time of the study (Dec 2021-Jan 2022).

3.1 UI mock-up walk-throughs

The UI mock-ups were designed according to the use case scenario described in Section 2.2 and based on earlier designs in the project PAPAYA [8]. In Figure 2, we present three screens from the UI mock-ups [1]. The first screen (Figure 2) features the "Consent form for participating in a study", which served as the starting screen of the walk-throughs on UIs. It is a multi-layered policy and consent form that informs users about how their data is protected if they click on extra links. When participants click on the link tagged with 'a' (letter tags are only for illustration purposes and not part of the UI) in the figure, they are directed to the second screen of Figure 2, which includes the functional description of functional encryption tagged as 'b'. Similarly, when clicking on the link tagged with 'c', participants will be directed to the third screen which includes the structural description of FE tagged as 'd'– the complete structural description UI is displayed in Appendix A.3. Our participants were told to act as users, who previously installed an app provided by a fictitious Telecom provider called *TeleCom AB*. The Telecom company would request their consent to share their data for conducting statistical analysis in a privacy-friendly way and share the results with a third-party (MediaSurvey).

The mock-up walk-throughs with focus group participants were conducted individually and in parallel. The walk-throughs served two purposes: the first was to allow participants to have a first-hand experience of the mock-ups, and the second was to collect data from their walk-through corresponding to their interests in different types and details of explanations of how their data are technically protected. All walk-throughs lasted approximately 5-10 minutes in total. The protocol of the walk-through is presented in Appendix A.1.

3.2 Focus group workshops

Participants of the UI walk-throughs joined the online focus group workshops after a short break. The four focus group workshops consisted of 3-4 participants each. According to their technical knowledge, we had two focus groups with lay users, and two with users having a technical background in cryptography. Mentimeter [26], which is an interactive presentation software was used to facilitate interactions and discussions with participants online, thus allowing them to respond to questions individually before the group discussions. The individual responses of participants prior to group discussions enabled individual reflection as well as possibly mitigated the conformity bias of the focus group. The workshop consisted of the following elements: 1) introduction to the workshop, setup and tools used for the workshop, 2) discussion on consent (related to the consent screen in Fig. 2) and incentives, 3) discussion on the perceived privacy functionality of the use-case, 4) discussion on the functional and structural descriptions and mental models, and 5) questions and discussions for analyzing the users' comprehensions.

The workshop ended with a questionnaire for demographics and reflections on the results of the study. Participants were offered a gift card as compensation, which was however not announced before the study was conducted to avoid biases (i.e. when discussing incentives). A detailed protocol can be found in Appendix A.

3.3 Data analysis

Data collected from the individual walk-throughs and focus groups were transcribed manually from recordings. For the walk-throughs, we specifically captured data relating to the clicking behavior through the user interface and comments made by the participants. The recordings of the walk-throughs were double-checked with the transcription. We provide the summary of the data in Section 3.5. The transcripts of the focus group workshops were analyzed according to the thematic analysis process [11]. The authors read and went through the transcripts as well as the recordings, and met regularly throughout the analysis process to discuss and resolve conflicts. One author was the moderator of all focus groups for consistency. Two authors coded the open data individually, then all authors met to discuss the results, resolve conflicts, and form the code-book. After iterative coding and merging of codes, all authors reviewed and agreed on the merging results in a workshop meeting. Next in the analysis was the categorization of the main and sub-themes, which was partially inductive, following the structure of the focus group's discussion elements. All authors met and agreed on the terminology and categorization of the themes and finalized the analysis in a final discussion workshop. An overview of themes and codes can be found in Appendix A.5.

3.4 Study A participants overview

There were 13 participants (p1-p13) who took part in the UI walk-throughs followed by the focus group (FG) workshops. There were three participants in each of FG0, FG1, and FG3, whereas there were four participants in FG2. Participants in FG0 and FG2 were recruited as lay users, and their responses to the questionnaire revealed that some reported having IT-related expertise (see Table 2 in Appendix A.4 for detailed responses). However, all FG0 and FG2 participants indicated their novice/inexpert responses to their expertise in cryptography. In contrast, FG1 and FG3 participants indicated competent/expert/proficient expertise in cryptography. Overall participants responded to the gender question with female (5), male (6), and prefer not to say (2). Six participants indicated they were in the age range of 18–29, two in 30–39, four in 40–49, and one in 50–59. Details are illustrated in Table 2 in Appendix A.4.

[1] UIs can be found using the link: https://adobe.ly/3Vs9VhU

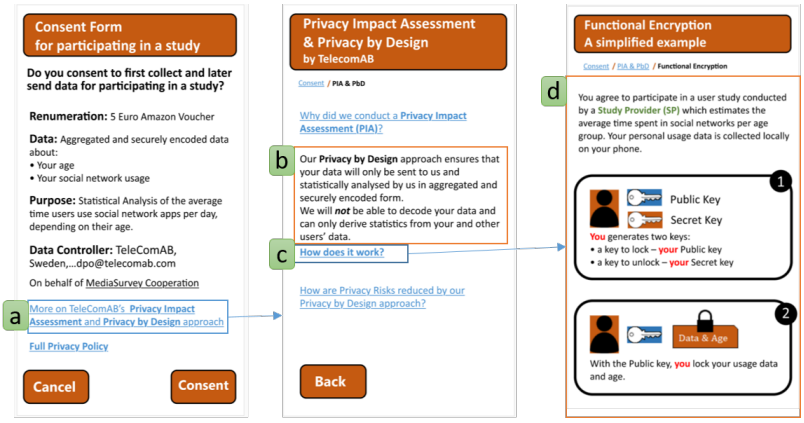


Figure 2: Three UI mock-ups in study A: consent, functional description, and the start of structural description

3.5 UI Walk-through results

Five participants (p2, p3, p5, p6, p7) clicked on the link tagged with 'a' in Figure 2 and on other links for exploring the mock-ups until they consented. They showed interest in viewing explanations on the privacy by design approach on the subsequent screens that were going beyond the short textual description "aggregated and securely encoded" on the first screen. However, they could have acted so because the study was conducted as a walk-through. All other eight participants clicked on 'Cancel' (2) or 'Consent' (6) without any observable interest in further privacy by design information beyond the short textual description.

3.6 Focus group results

The results of focus groups are presented under the following subsections (indicated in italics as themes and sub-themes).

3.6.1 Incentives and Data Sharing. All in FG0 and p10 in FG2 (4 in total) indicated yes to sharing their data in the scenario, however, in FG1 and FG3 participants were more skeptical to share. Furthermore, the incentive of a voucher or discount seems to dampen their willingness to share, where only one participant from FG0 indicated yes to sharing data in exchange for a voucher/discount.

Factors hindering sharing. Many participants (6) indicated that they responded out of a habit of not sharing their data, as p13 states "I would generally not contribute to participate with my data". Besides the unappealing monetary incentive (indicated by seven people) and the negative impression of sharing data in exchange for money (4) that is considered "suspicious", data privacy concerns as a result of sharing data appeared as an important hindering factor for participants (5). They indicated marketing, spam, and advertisements as possible consequences of sharing their data, as well as data leakage. Furthermore, p8 expressed a privacy concern stating "We will only have an increased possibility of tracking people, so I am a little bit concerned with that". Concerns about the specific brand of the incentive provider, i.e. Amazon (2), and lack of trust due to negative past online experiences (2) were other hindering factors for data sharing.

Factors motivating sharing. The participants emphasized the importance of transparency, privacy, and security considerations in motivating data sharing (3). Participants cited transparency of data processing, including whether data is anonymous, and reassurances regarding responsible data usage as their privacy considerations for sharing data. Additionally, improving anonymity by using more data due to aggregation was highlighted, as p5 explains: "if there are many people participating then everyone will be more secure because anonymity loves company". Participants answered a question on what incentives would motivate them to give their consent in the scenario (see Appendix A.2) and discussed incentives. Despite the variety of responses, all participants reported that the benefit of the common good can motivate the sharing of data. Sustainable and environmental issues were the most motivating incentives, followed by tracking COVID-19 cases, city planning and public transportation, and finally discounts and vouchers. Some participants (p5, p6, p12) specifically highlighted that their intention for providing their data for the common good was coupled with the requirement that privacy is preserved. The monetary incentive per se was perceived as an added value (5).

3.6.2 Perceptions of the addressed terminologies. In all focus groups, participants highlighted their preferences when it comes to suitable terminologies to be used for mediating (to different types of users) that TelecomAB cannot read/access the user data in "clear text". They were to choose between (1) "securely encoded data", (2)"securely encrypted data" and (3)"securely protected data" (see Appendix A.2).

Opinions and preferences – encrypted. It was revealed that 'encrypted' was preferred for the general public (p12 and p13), as p13 explains: "encryption is a word that is like becoming popular because it appears everywhere....like instant messaging systems like WhatsApp or like Zoom.... maybe it's becoming more well-known word, but My first thought was to avoid it". Besides encryption, many participants, especially those with technical background, believed that 'protected' is the better word to be used for communicating to the general public (FG1, p1, p3), as P4 states: " to suit for the most you need to choose protected because it will be easier for more people to understand it". Overall 'encrypted' was the most

preferred term by the majority of participants (FG0, FG1, FG2, p11, p13). Participants indicated that 'encrypted' gives the feeling of more safety or security (p2, p3), as p2 states: "encrypted for me is obviously number one to keep the data safe". " encrypted" was also deemed to be more professional (p7,p9), as p9 states: "because encrypted sounds more professional and even if users don't know exactly what it means it sounds professional enough". The use of 'encrypted' is perceived to be widespread which indicated its suitability (p12, p13), as p12 mentions: " I think encrypted is a word that we hear more and more in the general sense. You go to WhatsApp and see encrypted... now it's getting attention, so I think, like, the general audience know what encrypted means like in a very, very broad sense". Nonetheless, participants indicated concerns that 'encrypted' is too specific (p11) and that it can be misleading, as p13 explains "I just think encrypted, even though it's, like, a popular meaning, in this case, it can be misleading because according to the description, there's no reference to encryption here".

Opinions and preferences – protected. When discussing the protected word, P1 and P2 mentioned the sense of safety that is associated with 'protected' contrary to expert participants from FG2 who believed that 'protected' is the least suitable term that is unclear in meaning, as p10 adds: "protected seems... it's just a word that seems nothing technical".

Opinions and preferences – encoded. Participants had many concerns related to the term 'encoded', as it does not sound reassuring, nor is associated with security (FG0, p5, p6, p12, p13). The participants from FG0 explain: "Encoded, for me it sounds like something that somebody can uncode it" (p2), "... my mind goes to when you encode videos and stuff. And I don't really associate it with security, the encode word. So that's why I picked it last" (p3). On the other hand, p11 preferred the term by stating: "I think that the encoded and possible encrypted, mostly encoded, would be more suitable. And even if it does not- I think that people would not understand what encode really means but they would understand some general meaning and so in fact its board enough, its imprecise enough I think in peoples mind in order to mean whatever they want it to mean".

3.6.3 Descriptions preferences and feedback. Participants were asked which description they preferred (we referred to description b in Figure 2 as description 1 which is the functional explanation and description d as description 2 which is the structural explanation).

Structural description appreciated. All in FG1 and FG3 (experts) preferred the structural description (description 2). However, fewer lay participants in FG0 (p2 and p3) and FG2 (p7) chose the structural description. Participants were asked to elaborate on their reasons for the description they preferred. The visual appeal of the structural description was appreciated in terms of using graphics and images (p2, p3, p5, p6, p13), as p13 stated " visual description is more, how do you say, enticing? So, it's like something graphical to see and follow and it makes it much easier. That is why I prefer the graphical use". The step-by-step illustration was perceived to have a good impact on explaining functional encryption (p3, p4, p5, p6). Expert participants also appreciated the technical details provided by the structural description (p5, p6, p7, p11, p12). They perceived the technical details provided by the structural description and the step-by-step explanations as better understandable and more trustworthy: "You show me how you do it and then I buy it because I know what you are doing. I can trust your design is correct" (p12). Also, p5 noted: "...it goes things through step by step sort of how does it work? that's the sort of description I would always prefer because it says something, it can give the reader something to relate to and actually understand". The structural description "gives the feeling to the user to understand what's happened behind the words of the description one" (p4). As both p4 and p5 pointed out, the functional explanation can be perceived as 'scary' when it simply includes claims without much explanation compared to the structural explanation, which describes what's happening and therefore can be less frightening. P3 further added that smaller sections are easier to read on the phone, and stated that "the illustrations also help for the inexperienced people who haven't gotten knowledge about encryption to kind of get a picture of how it works" and "...I would like to know what that's all about".

Functional description preferred. The remaining participants of FG0 and FG2 (p1, p8, p9, p10) preferred the functional description (description 1). There was an appreciation for the brief format of the description which was quicker to read (p1, p9). P9 indicates the probability of confusion otherwise stating: "I don't think many users would actually read the step-by-step to understand how exactly their data is changed and analyzed and everything. Because it's more confusing than just a short text that says this and this and this". Some participants considered the description to be sufficient for addressing the main points (p8, p9, p10).

Combination of both descriptions preferred. The preference for a combination of both descriptions was voiced by participants (p1, p7, p8, p10), as p10 states " I think it is in fact complimentary. It's good to have a first description very small one and then if people want to have more information they can click on the second one which will be more detailed".

3.6.4 Comprehensions of FE. Similar to previous stages of the workshop, participants responded individually to the four comprehension questions prior to the group's discussion. Below is the summary of the correct responses to each question, followed by themes relating to the discussions of participants' answers to the questions.

Understanding Telecom AB only gets encrypted user data. In the first question "From the data that the user contributes to the study, do you think that TeleCom AB can directly see the user's social network usage information?", the majority (6) answered "unsure", with five answering correctly as follows:

- Yes (p7, p12)
- No (p2, p3, p5, p6, p9) [correct answer]
- Not sure (p1, p4, p8, p10, p11, p13)

Participants who answered correctly referred to the description text (p2, p3, p5, p6, and p9). One participant (p2) reasoned that they need to give permission first, while p3 stated "I think they mentioned before that they could not access your data because they did not have the encryption key for it". However, while the second answer was meant to be the correct one, some of the expert participants that gave a different answer were considering possible risks for the application scenario and therefore also provided correct

justifications for their answers. For instance, p4 pointed out that if she was the only one sharing her data "... at the end the average will be my result" (in other words: the answer would depend on the anonymity set size). And p12 expressed that a telecom provider anyhow already had (meta) data about the social media usage, and hence it would not matter if the data were encrypted or not.

Understanding only data sent is securely 'encoded'. For the second question, "Which data do you think is securely encoded?", the majority of participants (4 out of 7 lay users and 5 out 6 experts) answered correctly as follows:

- The data sent by the user to TeleCom AB (p1, p2, p4, p5, p7, p10, p11, p12, p13) [correct answer]
- The statistical analysis result that TeleCom AB produces
- Both (p3, p6, p9)
- None (p8)

Some of the participants (p1, p3, p7) assumed and discussed that the statistical analysis result would not leak personal information or would be anonymous and for that reason was not encrypted, and as p1 stated: "Usually, just an aggregation of the data and there is no way to pinpoint specific thing that could be linked to users so there is no need to encrypt that data unless it's highly confidential". P3, who first (wrongly) stated that the data was encrypted by Telecom AB (note: it is actually encrypted by the user's phone), then mentioned that the (statistical analysis) data "becomes indirectly encoded securely because they can't be traced back to you once it's analyzed".

Understanding that others cannot decrypt user data. For the third question, "Do you think that someone can de-code/decrypt/access the data, that the user sends, in clear text, if so, then who?", only a few participants, mainly expert users (5 out 6) and one lay user, had correct responses as follows:

- TelecomAB (p1, p2, p3, p7, p13)
- MediaSurvey Cooperation that requests the result
- Both (p8)
- None (p4, p5, p6, p9, p11, p12) [correct answer]

After showing the functional descriptions to the participants, we repeated the third question. However, none changed their answer. Nevertheless, three experts (p5, p11, p12) from FG2 and FG4 mentioned that the short functional description alone may not express clearly this property. Again, p5 emphasized that it was the structural explanation that led to his answer and not the functional one. The functional description "was just this little piece of text. That one, if only would have had that one, I would have answered differently." The discussion revealed several misunderstandings about functional encryption and its ability to analyze data in encrypted form. Specifically, it was stated that in order to analyze data, they have to be decrypted, as p1 highlighted that "they cannot analyze the text that they get if they cannot decrypt it, and they cannot decrypt it without being able to unencrypt it and access it", and p13 stated that "if we assume that you give them the right to statistically analyze the data it means that you have given the key at least to decrypt part of the data that was sent". In total, our comprehension questions and discussions revealed that participants in the focus groups did not correctly understand all facts that our functional and structural explanations tried to convey. However, especially for the second and third questions, expert participants, to a larger extent, could provide correct answers and/or well-grounded reasons for their chosen answers.

4 STUDY B: ONLINE SURVEY

4.1 Hypotheses

Based on the results of Study A, we derived three hypotheses for Study B. As reported in Section 3.6.3, all experts and only two lay participants preferred the structural explanation of FE, and the remaining lay participants preferred the functional one. Therefore, we consider that there could be a difference, between lay and experts, regarding their opinions and satisfaction with different types of explanations (H1). Furthermore, as reported in Section 3.6.1, participants who said yes to sharing their data in the scenario (all in FG0 and one in FG2) were from the lay FGs, meanwhile, experts were more skeptical to share their data. It was also emphasized to a greater extent by expert participants that they preferred the structural explanation since they considered it to be more trustworthy. Considering the difference in their decisions to share data and their preferences for the types of explanations, we decided to test H2. Finally, participants' answers to the comprehension questions, especially the third question, revealed that experts understood how FE works better to a large extent than lay participants. Expert participants claim that mainly the structural explanation contributed to their understanding and laypersons might have preferred the functional explanation because they found it more understandable among other reasons. In the focus groups, we could not conclude whether the comprehension of FE was the result of the structural or the functional explanation (because participants in FGs saw both), therefore we decided to test H3,

- **H1.** There is a difference in users' satisfaction with (H1-1) and opinions on (H1-2) the descriptions based on the types of explanations, either functional or structural, they receive and their expertise (concerning encryption as we defined in our study, see Section 4.2), either lay or expert.
- **H2.** There is a difference between users' decisions on sharing their data based on the types of explanations they receive and their expertise.
- **H3.** There is a difference between users' comprehension of how FE works based on the types of explanations they receive and their expertise.

Study B is an online survey conducted with participants recruited through Prolific, an online platform for recruiting and managing participants [27]. We used Prolific filters to recruit people whose current countries of residency were EU countries, EEA countries, the UK and Switzerland due to the scope of our funders. To test our hypotheses derived from the results of our focus groups (see Section 4.1), we distinguish between expert and lay participants in terms of their knowledge of encryption. Therefore, instead of relying on subjective and self-reported measures for participants' expertise in encryption, we conducted a prescreening study to categorize participants in preparation for the survey. The prescreening study categorized prospective participants, based on their answers into expert and lay groups. We then invited the expert and lay participants to take part in the main survey. We first report on the design of study B including the details of the prescreening study,

main survey and measurements and then we present the results of our survey.

4.2 Prescreening study

After obtaining consent, participants were asked three encryption-related questions about symmetric, asymmetric, and functional encryption as follows (correct answers italicized).

(1) Which of the following statements is TRUE for symmetric encryption? (Options: a) The encryption key is symmetric. b) The decryption key is secret, but the encryption key is not. *c) Both the encryption and the decryption keys are secret.* d) The encrypted message is symmetric.)
(2) Which of the following statements is TRUE for public key encryption (asymmetric encryption)? (Options: *a) The encryption key can be published.* b) The key for decrypting an encrypted message is publicly decrypted. c) Both the encryption and the decryption keys are public. d) The encrypted message is not symmetric.)
(3) Which of the following statements is TRUE for functional encryption? (Options: a) In contrast to homomorphic encryption, a mathematical function is encrypted. b) In contrast to homomorphic encryption, the result of a function calculated on encrypted text can be made available in encrypted form. *c) In contrast to homomorphic encryption, the result of a function calculated on encrypted text can be made available in clear text.*)

Note that all the questions had two extra options as well: "None of the above" and "I do not know/I am not sure" and we instructed participants at the beginning of the study not to guess the answer and instead indicate that they did not know or were not sure.

As we aimed to explore the implications of FE explanations, we excluded participants who already knew what FE was thereby answering the last question correctly. Participants who answered any of the first two questions correctly were classified as knowledgeable in encryption (herein experts) and the ones who answered all questions incorrectly were classified as laypersons. Time and resource limitations did not allow us to limit the sampling to those who correctly answered both questions on asymmetric and symmetric encryption. Likewise, for the same reason, we started recruiting participants among people who possessed at least a bachelor's degree in a computing field (more specifically, Computer Science, Computing (IT), Engineering, and Mathematics) because we assumed that the chance of finding knowledgeable people about encryption would be higher. The first 700 samples had a university degree in one of the mentioned fields. To make the sample more diverse regarding the field of study and the educational background, the last 300 participants were recruited without any restrictions on their educational degrees and we excluded people who had a background in any of the computing fields mentioned above.

In total, we recruited 1000 participants, on Dec 2021, for our prescreening study which resulted in 403 participants categorized as experts (283 answered either of the first two questions correctly and 120 answered both correctly) and 464 as lay persons who got invited to take part in our survey. The estimated time for taking part in the prescreening study was three minutes and participants were compensated accordingly (see Ethical considerations under Section 3).

4.3 Main survey

The online survey consisted of four parts: 1) introduction to the study (on the Prolific website) and request for consent (on the university's survey platform compliant with its policies), 2) demographic questions, 3) main survey content and questions, and 4) closing session with extra questions.

The third part, the main survey content, included: a) introduction to a specific privacy-preserving data analysis scenario, b) pre-explanation decision-related questions, c) exposing users to the explanation of FE (either functional or structural) as the specific mechanism used to preserve users' privacy in the scenario, d) post-explanation decision-related questions, and e) comprehension and satisfaction-related questions. The scenario and the FE explanations in our survey were almost the same as the ones used in our focus groups. Nonetheless, based on our participants' feedback and comments in our focus groups and to be able to investigate the effects of each explanation (not a combination of both contrary to how they got exposed to explanations in focus groups) on users' comprehension, decisions, and satisfaction, we adapted our explanations and also made changes in terminologies we used (see Section 3.6.2). Appendix B shows the survey guide including the scenario description and functional and structural explanations in addition to the questions asked in our survey. Almost half of the experts and half of the lay participants were invited to take part in our online survey with the functional explanation and the other halves with the structural explanation of FE.

347 out of 403 experts and 370 out of 464 laypersons successfully completed the survey on Jan 2022. The demographic questions included age, gender, the highest education level, and the field of study, if applicable. The estimated time to finish the survey with the functional explanation was 9 minutes and the structural one was 10 minutes and participants were compensated accordingly (see Ethical considerations under Section 3)).

In the closing session, participants answered two standardized questionnaires. First, they answered a questionnaire measuring their general privacy concern level taken from the Internet Users' Information Privacy Concerns (IUIPC) scale [25]. Then we presented participants with 10 statements aiming to measure rational and intuitive decision-making styles obtained from Hamilton et al. [19]. Afterward, we thanked the participants and gave them a completion code with which they got compensated on the Prolific website given the fact that they already answered the attention question correctly in the survey.

4.4 Measurements and data analysis

We conducted both qualitative and quantitative data analysis to analyze the data collected in our survey. The analysis of the qualitative data collected in the survey followed a similar process described in Section 3.3. However, data were inductively analyzed based on the themes of the focus group workshops. In our quantitative analysis, we have two main independent binary variables: type of the explanation (structural versus functional) and the level of expertise in encryption (expert vs lay). We have four main groups of dependent

variables to assess: 1) satisfaction with the descriptions, 2) opinions on the descriptions, 3) comprehension of how FE works based on the description, and 4) change in decisions of sharing data. To assess users' satisfaction with FE explanations to which they were exposed in the survey, we had four five-point Likert-scale questions in regard to the level of details (LOD), presentation (PRS), length (LNG), and wording/terminologies (TRM) (see Appendix B.4). We used the means of these four variables to measure overall satisfaction (OSAT) (see Section 4.6.1 for justification of using the means of the aforementioned variables to measure the overall satisfaction). In addition, we gauged users' opinions on different aspects of explanations using seven five-point Likert-scale questions related to the extent of understandability (UND), convincibility (CNV), trustworthiness (TRW), easiness to read (ESR), and helpfulness in giving informed consent for sharing data (in the scenario) (MIC).

To assess comprehension, we developed a quiz-like questionnaire consisting of four questions (see Appendix B.4). The questions aimed to assess general comprehension of how FE works in the context, i.e. the information provided in the descriptions regarding what data is encrypted, who can decrypt data, and who can access the results of data analysis in plain text. The overall comprehension variable (OCMP) shows the number of comprehension questions correctly answered.

Finally, to assess the impact of FE explanations on users' decisions to share their data we defined a change-in-decision variable (CHNG) which distinguishes between the number of changes that ended up as definitive answers, either as YES or NO, compared to other types of changes. In other words, CHNG variable has three categories: a) a *change* in answer from anything other than a Yes answer to a Yes answer after getting exposed to the FE explanation, b) a *change* in answer from anything other than a No answer to a No answer, and c) any other combinations (for example, from a Yes/No to an "Unsure/I do not know" answer). Different statistical methods were used to analyze the data and test the hypotheses, including descriptive statistics and more complex statistical models. When statistical tests were used, the related assumptions were first checked and if met we proceeded with the analysis.

4.5 Participants' demographics

347 experts (175 who experienced the functional explanation and 172 who were exposed to the structural one) and 370 lay participants (190 who experienced the functional explanation and 180 who were exposed to the structural one) completed study B, our online survey. Table 1 shows the demographics of our survey participants and the total number of them in each group (L-F group: Lay participants receiving Functional description, E-F group: Experts receiving Functional description, L-S: Lay participants receiving Structural description, and finally E-S group: Experts receiving Structural description). As described in Section 4.2, to increase the chance of finding expert participants we recruited the first 700 samples of our prescreening study from people who had at least a bachelor's degree in a computing field which explains why the participants who identified themselves as males significantly outnumbered the ones who identified themselves as females and 74% of our participants had graduate or undergraduate degrees. The majority of participants were below 40 years.

4.6 Results

In the following subsections, we report on the results of our data analyses conducted to check the hypotheses reported in Section 4.1. Section 4.6.1 reports different opinions and satisfaction with the two explanations. Section 4.6.2 presents the analysis related to the impact of explanations on users' decisions and Section 4.6.3 reports the results related to different users' comprehension of FE based on the explanations.

4.6.1 Users' opinions of explanations. As described in 4.4, the overall satisfaction score is the mean of four scores (each score is a number between 1 (strongly disagree) to 5 (strongly agree)) that participants gave to four different statements about different aspects of satisfaction including satisfaction with the level of details (LOD), presentation (PRS), length (LNG), and wordings/terminologies (TRM) in an explanation (see Appendix B.4). We used Principal Component Analysis (PCA) with Varimax rotation to assess whether the four items load correctly into one factor. The KMO measure of sampling adequacy was acceptable, 0.783, and Bartlett's test of sphericity was significant, p < 00.1. We also checked the reliability of the scale and Cronbach's alpha = 0.822 which indicates a good level of internal consistency between the measures used to calculate our satisfaction scale.

No significant differences were found between laypersons and experts in general regarding their overall satisfaction with the explanation (OSAT) they received or within each group exposed to a specific explanation type (functional vs structural). However, people who were exposed to the structural explanation had higher overall satisfaction scores (OSAT) ($Meanrank = 388.94$) compared to people who were exposed to the functional explanation ($Meanrank = 330.12$), regardless of their expertise. A Man-Whitney U test showed that the difference was significant, $U(N - functional = 365, N - structural = 352) = 74780,50, z = 3.84, p < 0.001$. In the same way, within both expert and lay groups, people who were exposed to the structural explanation gave much higher overall satisfaction rates compared to people who were exposed to the functional explanation (note that the results of Man-Whitney U tests conducted within each subgroup are omitted due to space limitations). Therefore, the null hypothesis of H1-1 is partly rejected and H1-1 partly retains (for the difference based on the type of explanations). It means that the overall satisfaction with the structural description is higher, regardless of the level of expertise.

Experts and laypersons in general did not differ significantly in their subjective opinions on the understandability of the explanation (UND) they received, the explanation's invincibility (CNV), trustworthiness (TRW), and how helpful it was in data-sharing decisions (MICS). In addition, within each specific group of explanations (functional versus structural), there was no significant difference between the aforementioned scores based on expertise. Nevertheless, experts' and layperson's opinions on explanations differed based on the specific type of explanation, as explained below:

The subjective understandability score of the structural explanation was higher ($Meanrank = 373.24$) than that of the functional explanation ($Meanrank = 345.27$), regardless of the expertise of the people who scored them. A Mann-Whitney U test shows that this difference is significant, $U(N - functional = 365, N - structural =$

Table 1: Demographic information of survey participants (L= Lay, E= Expert, F= Functional, S= Structural).

Demographic info	L-F, n= 190	E-F, n= 175	L-S, n= 180	E-S, n= 172	Total, n= 717
Gender					
Female	79	52	78	57	266
Male	106	121	98	113	438
Other	5	2	3	2	12
Preferred not to say	0	0	1	0	1
Age					
18-24	115	90	116	104	425
25-39	70	76	59	63	268
40-65	5	9	5	5	24
66+	0	0	0	0	0
The highest education level (Levels similar to what Prolific offers)					
Secondary education (e.g. GED/GCSE)	5	3	2	5	15
High school diploma/A-levels	38	21	46	22	127
Technical/community college	11	11	13	8	43
Undergraduate degree (BA/BSc/other)	97	77	84	93	351
Graduate degree (MA/MSc/MPhil/other)	39	60	35	44	178
No answer to the related question	0	3	0	0	3
Level of privacy concerns [25]					
Mean	3.37	3.42	3.36	3.47	3.40
Std. Deviation	0.51	0.51	0.55	0.52	0.52
The score of rational decision-making style [19]					
Mean	4.02	4.18	4.11	4.14	4.11
Std. Deviation	0.46	0.48	0.52	0.52	0.50
The score of intuitive decision-making style [19]					
Mean	2.76	2.64	2.57	2.66	2.66
Std. Deviation	0.67	0.78	0.72	0.70	0.72

352) = 59227.00, $z = -2.045, p = 0.041$. As well, in both expert and lay groups, people who were exposed to the structural explanation gave it a much higher understandability score (UND) compared to people who were exposed to the functional description. Nonetheless, the score for being easy to read (ESR) did not differ significantly for the functional and structural explanations regardless of the expertise of the people who scored them.

Likewise, the convincibility score of the structural explanation was higher ($Meanrank = 401.51$) than that of the functional explanation ($Meanrank = 318.01$), regardless of the expertise of the people who scored them. A Mann-Whitney U test shows that this difference is significant, $U(N-functional = 365, N-structural = 352) = 49278.00, z = -5.736, p < 0.001$. In both expert and lay groups, people who were exposed to the structural explanation also gave it a much higher convincibility score (CNV) compared to people who were exposed to the functional description.

Similarly, the trustworthiness score of the structural explanation was higher ($Meanrank = 392.30$) than that of the functional explanation ($Meanrank = 326.89$), regardless of the expertise of the people who scored them. A Mann-Whitney U test shows that this difference is significant, $U(N-functional = 365, N-structural = 352) = 52520.00, z = -4.476, p < 0.001$. Similarly, in both expert and lay groups, people who were exposed to the structural explanation gave it a much higher trustworthiness score (TRW) compared to people who were exposed to the functional explanation.

The structural explanation is also assumed to be more helpful for making data-sharing decisions ($Meanrank = 389.27$) than the functional explanation ($Meanrank = 329.81$) based on analysis of MIC score, regardless of users' expertise. A Mann-Whitney U test shows that this difference is significant, $U(N-functional = 365, N-structural = 352) = 53586.50, z = -4.352, p < 0.001$. Likewise, in both expert and lay groups, people who were exposed to the structural explanation further gave it a much higher MIC (helpfulness in making data-sharing decisions) score compared to people who were exposed to the functional explanation.

Consequently, the null hypothesis of H1-2 is partly rejected and H1-2 partly retains (for the difference based on the type of explanations). It means that people find the structural descriptions more trustworthy, understandable, convincing, and helpful in making data-sharing decisions, regardless of their level of expertise in encryption. The participants categorized as experts in our survey had a slightly higher level of privacy concerns (not statistically significant) compared to lay participants ($L-Mean = 3.36, L-SD = 0.53, E-Mean = 3.45, E-SD = 0.51$). Nonetheless, being more concerned about privacy did not lead to a significant difference between experts and laypersons in their opinions on and satisfaction with the different types of descriptions. People's behaviors when making decisions may not necessarily abide by their subjective opinions on a specific description. Is the structural description really more helpful in making informed decisions? We will investigate it in Section 4.6.2.

4.6.2 Impact of explanations on users' decisions. Generally, lots of experts and lay participants were persistent in their decisions to share or not to share their data in the scenario. In other words, the FE explanation they received did not affect the definitive decisions they initially made regarding whether to give their consent. Almost 47% of lay participants, regardless of the explanation they received, kept their previous decisions of giving their consent to share their data (90 out of 190 in the L-F group and 84 out of 180 in the L-S). Similarly, 47% of the E-F group (83 out of 175) and 49% of the E-S group (84 out of 172) were rigid in their decision to share their data after receiving the explanation. On the other hand, a few percentages of participants in all groups, approximately 10%, initially decided not to share their data and did not change their decision (L-F= 20 (out of 190), L-S= 20 (out of 180), E-F= 20 (out of 175), E-S= 16 (out of 172)).

However, not all decisions before and after receiving structural or functional explanations were unvarying definitive decisions. While some of the participants could not make definitive decisions

both before and after receiving the FE explanation (i.e. they were persistent in their doubts on whether or not to give consent: 20 in the L-F group, 9 in the L-S group, 11 of the E-F participants, and 13 in E-S group), some of them changed their definitive decisions, for example, a no to yes, a yes to no, or a definitive decision to a doubting one (23 in L-F, 31 in L-S, 31 in E-F, and 28 in E-S) and some made a definitive decision although initially they did not (37 in L-F, 36 in L-S, 29 in E-F, and 37 in E-S).

The ultimate goal of providing users with transparency on underlying privacy-preserving technologies used to protect their data is to help them make informed decisions. An informed decision is a definitive decision. Therefore, we investigated the differences between groups regarding their definitive decisions. In general, after receiving the explanations, the number of definitive decisions increased (from 530 to 610 out of 717). More participants agreed to share their data (from 376 to 502) and fewer refused to give their consent (from 154 to 108). More specifically, from 190 participants in the L-F group, 10 changed their decision to a definitive No and 35 changed their decision to a definitive Yes while the rest either were persistent in their initial decisions or did not make a definitive decision. Among 180 participants in the L-S group, four changed their decision to a definitive No and 48 changed their decision to a definitive Yes. Out of 175 people in the E-F group, 14 changed their decision to a definitive No and 32 to a definitive Yes. Finally, out of 172 people in E-S, four changed their decision to No and 46 to Yes.

There was no evidence of a significant association between expertise and the CHNG variable (making definite decisions) in general and within each group of explanations. However, a Chi-Square Test of Independence showed significant evidence of association ($\chi^2(2, 717) = 13.396, p = 0.001$) between CHNG variable and the type of explanations regardless of the level of expertise. A Dunn-Bonferroni post hoc comparison test revealed that the number of people who changed their decisions to Yes (from any initial decisions) is significantly higher for people who were exposed to the structural explanation. Also, the number of people who changed their decisions to No is significantly lower for people who were exposed to the structural explanation (adjusted $p < 0.008$). Therefore, the null hypothesis of H2 is partly rejected and H2 partly retains (for the difference based on the type of explanations). People who get exposed to the structural explanation are more likely to make a definitive decision and consent to share their data regardless of their level of expertise. Our expert and lay participants are both more rational decision makers than intuitive decision makers as the scores in Table 1 show. Experts have an average rank of 380.32, while lay participants have an average rank of 339.01. A Man-Whitney U test shows that this difference is significant ($U(N - experts = 347, N - non - experts = 370) = 56797.50, z = -2.70, p = 0.007$.). However, being more rational did not lead to a significant difference between experts and laypersons in making definitive decisions after receiving FE explanations.

Reasons behind different choices. The most-selected reason by both expert and lay participants for giving consent (making a definitive decision of yes to consent) before they received any FE explanation by far was receiving the monetary incentive. However, the results revealed that the explanations positively affected users' perception of their data privacy. After getting exposed to the explanations, the most-stated reason was taking into consideration that privacy protection and security were in place and the perception of privacy and safety, either due to security and privacy protection mechanisms in place, or that they do not perceive privacy risks in the context. However, privacy and security concerns and skepticism about privacy protection did not fade by the explanations provided. *Not usually giving consent in general* was the most-selected reason for disagreeing to give consent closely followed by concerns about privacy and security of data, and having doubts about the third party (MediaSurvey Corporation) for both experts and lay participants, before receiving the explanations. The most-stated reasons for not giving consent remained quite the same after receiving extra information on the underlying privacy mechanism. Participants mainly highlighted their personal discomfort and attitudes toward not consenting and specifically referred to their concerns for the privacy of their data and their skepticism of privacy protection and their concerns for the third party. Having doubts about the security and privacy of their data and having doubts about the third party were also the most-selected reasons by experts and laypersons who did not make definitive decisions before receiving any explanation on the underlying privacy-preserving technique. Privacy and security concerns including skepticism and lack of clarity about privacy protection and concerns about the third party remained the most-stated reasons behind the choices that were not definitive after receiving FE explanations.

4.6.3 Impact of explanations on users' comprehension. We asked four comprehension questions (see Appendix B.4). The questions asked covered the core features conveyed in the explanations regarding FE. In other words, the questions investigate users' understanding of which entities (e.g. the controller, TeleCome AB, and the third party, MediaSurvey) could access which type of data and the results of statistical analysis conducted on the data, i.e. in plain text or in an encrypted format. Out of four comprehension questions we asked about how FE works from our participants, lay and expert participants who received the functional description answered on average 2 and 2.4 questions correctly in order while only 1.5 and 1.6 questions on average were answered correctly by lay and expert participants who were exposed to the structural description.

Regardless of their encryption expertise, the overall comprehension of FE (OCMP) for people who were exposed to the functional explanation of FE is higher ($Meanrank = 416.90$) than for people who were exposed to the structural explanation ($Meanrank = 298.96$). A Mann-Whitney U test shows that this difference is significant, $U(N - functional = 365, N - structural = 352) = 43107, z = -7.91, p < 0.001$. Likewise, in both expert and lay groups, people who were exposed to the functional explanation answered much more comprehension questions correctly compared to people who were exposed to the structural explanation. The results further revealed that experts who were exposed to the functional explanation could better comprehend how FE works ($Meanrank = 198.09$) compared to laypersons who were exposed to the functional explanation ($Meanrank = 169.10$). A Man-Whitney U test shows that the difference between experts' comprehension of functional explanation and of laypersons' is significant, $U(N - expert - functional = 175, N - layperson - functional = 190) = 19265.5, z = 2.71, p = 0.007$. Experts' and laypersons' comprehension of FE was not significantly different for the group exposed to the structural explanation.

Therefore, the null hypothesis of H3 is partly rejected and H3 partly retains (for the difference based on the type of explanations and the difference based on expertise if exposed to the functional description). It means that the functional description is generally more effective than the structural one in helping people, either expert or lay participants, to understand how FE works. However, when exposed to functional descriptions, experts have a better understanding of FE than laypersons which confirms the need for more tailored functional explanations to meet average users' needs.

5 DISCUSSIONS

The key findings of our two studies in relation to our research questions can be summarized as follows: Our focus groups showed that most participants preferred the precise technical term 'encrypted' in the description. Expert participants preferred structural explanations, while most non-expert participants preferred the functional one. The survey showed that independent of their expertise, people found the structural explanation more trustworthy, convincing, helpful for decision-making, and understandable (RQ1). Moreover, people that received the structural explanation are more likely to make a definitive decision and to agree to share their data (RQ2). While the perceived comprehension of FE was higher for those that received a structural explanation, the survey also revealed that independent of the expertise the overall objective comprehension of FE was actually higher for people that were exposed to the functional explanation (RQ3).

5.1 Users' preferences, interests, and habits

Data sharing interests and privacy. Focus groups with participants having technical backgrounds (FG1 and FG3) were more skeptical about sharing their data than the other groups with lay participants (FG0 and FG2). Sharing for the benefit of the common good was mutual among all participants, especially for sustainability reasons. Nevertheless, three participants indicated their agreement to share for the common good is coupled with the requirement of preserved privacy. Monetary incentives and direct benefits (e.g., services, better quality results) to users were indicated as motivating factors. However, monetary incentives were perceived as a 'red flag' by some and had the opposite effect on sharing. Similarly, in the survey, participants indicated the sharing tendency for the common good. However, participants' appreciation of the monetary incentives was significant. Unlike the focus groups, survey participants were responding anonymously to the survey, which might have been a contributing factor to this observation. Alternatively, the sample group could be biased since they were paid to participate in the study, unlike the focus groups where participants were not offered incentives prior to their participation in the study. We see that offering monetary incentives to users is perceived differently, and thus should be done by practitioners given privacy is preserved.

Preferences for precise terminologies. The results of our focus groups show distinct preferences for the terminologies used for describing technical attributes. Participants indicated preferences for self (being (non-technical) or for the general public. Although a few participants with technical backgrounds indicated the use of terms such as 'protected' for the general public, participants with non-technical backgrounds indicated otherwise. Our findings support recent work which shows that encryption, as a (meanwhile) well-understood term, is a useful privacy indicator and has outperformed other lay term descriptions [2, 16]. Similar to our results, related work shows that experts may underestimate non-expert technical knowledge [24]). Our results show a wide acceptance of using precise technical terms such as 'encrypted' over abstract terms like 'encoded' and 'protected' in connection with easy-to-understand explanations, especially since the encryption term is already commonly used for modern applications. Therefore, in this case, we recommend using the precise technical term for communicating technical terminologies to users coupled with usable explanations.

5.2 Implication of explanations on comprehensions and decisions

Some participants in study A, who did not answer comprehension questions correctly, had misconceptions about functional encryption and data analysis and particularly did not understand that data analysis could be conducted on encrypted data. These misconceptions about data analysis on encrypted data often stem from users' existing mental models, e.g. also observed by [5]. In contrast, participants who answered correctly often referred to the descriptions as a reason for their answers. It appears that the information provided in the descriptions was deemed useful for participants' comprehension. Especially expert participants who mostly answered the comprehension questions correctly and emphasized that they perceived the structural explanation as more understandable and trustworthy. However, we were not able to pinpoint which description really contributed to the participants' comprehension in study A, as the participants were exposed to both explanations. In contrast, the results of study B revealed that participants who were exposed to the functional explanation understood how FE works significantly better than those exposed to the structural description regardless of their expertise. We expected participants who understood better how FE works (the ones who were exposed to the functional explanations) to make more definite decisions about sharing data in the scenario than those who did not but this was not the case. The survey results revealed that more than half of the participants (approximately 58%), were persistent in their responses, i.e. definitive decisions, despite the explanations provided. Therefore, the contents and formats of the explanations did not seem to play a role in their decisions. This was similarly observed in study A where participants had a significant volition to consent/reject sharing their data regardless of the explanations provided. This poses a challenge to designers and developers of privacy notices who rely on improving transparency to protect users' privacy, especially for those who choose to share without being informed of the consequences. The majority who made persistent definite decisions in Study B agreed to share their data. Nevertheless, we also observed that explanations affected the decisions of a considerable amount of participants (35%) and the number of definitive decisions increased, and more participants agreed to share their data. In this regard, the survey results exposed the significant role of the structural explanation in increasing the number of people who agreed to share their data regardless of their expertise. However, as discussed before, people understood the functional explanation much better than the

structural one which raises the potential problem of privacy theatre. Privacy theatre dictates that PETs may provide the "feeling of improved privacy while doing little or nothing to actually improve privacy" [21]. The privacy theatre problem regarding the explanations of how a privacy mechanism works is also reported by Smart et al. [30], who investigated whether explanations of differential privacy that hid important information about algorithm parameters persuaded users to share more data. Their results revealed that the explanations had little effect on individuals' willingness to share data and most of their participants made up their minds about whether or not to share before they even learn about privacy protection regardless of whether they were offered the protection of differential privacy.

5.3 Discrepancy and the consequences

Although the information provided in the descriptions was useful for participants' correct comprehension in study A, we were not able to pinpoint which description contributed to their understanding. We only report on their preference, which was the structural explanation for most of the participants. Nonetheless, study B shows that there is a discrepancy between what is more satisfactory, and assumed to be more understandable and helpful in decision-making, and what actually users comprehend and how they eventually make a decision. The structural description was perceived to be more convincing, understandable, trustworthy, helpful in making decisions, and satisfactory. Furthermore, it was appreciated because of its presentation and level of detail. However, actual comprehension of how FE works and perception of correct data access was better for people exposed to the functional one regardless of their expertise.

Our study thus supports previous findings that recommend using functional explanations for crypto-based privacy technologies (in the form of E2EE) for forming correct mental models [32]. In addition, we provide insight that this recommendation is not limited to laypersons but rather should apply to all users regardless of their level of expertise. Furthermore, previous studies have shown the desire of technical users [24] or of other types of stakeholders [5] to have access to technical descriptions and details for establishing trust in a PET. These results correspond with our findings that structural explanations can still play an important role. However, our results further suggest that, in the case of FE, this may apply to both users with technical expertise and laypersons. Therefore, our results indicate that both descriptions are required in combination to serve satisfaction, comprehension, trustworthiness and decision-making. Using a multi-layered policy design, the functional explanation can be presented on an upper layer, while more details with a structural explanation can be provided as a link or on a lower layer. Providing the structural description alone or at the first and the functional description at the second layer can serve as a dark pattern because people may get easily convinced and make positive definitive decisions while they are satisfied without understanding the privacy-enhancing functionality.

5.4 Limitations

The binary categorization of users into expert and layperson groups in our study may be a limitation, given that users would potentially not fall under the binary classification but rather into a spectrum. We recruited experts in study A with the criteria for having knowledge in encryption but not in FE, and further validated it in the post-FG questionnaires (see Table 2 in Appendix A.4 for results). Laypersons (in study A) were recruited as not having any knowledge of cryptography, but it was revealed later that a few laypersons had some technical knowledge of IT. Hence, our lay participants were 'lay' in the domain of cryptography but not necessarily 'lay' in terms of IT knowledge. Similarly, in study B, we used knowledge of cryptography as the criteria for categorizing participants into expert and layperson groups. The questions were designed specifically for our study and were validated by two cryptography (more specifically FE) experts. Users were categorized as experts if they could answer at least one of the two screening questions correctly, but not the question on FE (details in Section 4.2). Even though the difference between some of the experts (who only answered one question correctly) and non-experts may not have been as large, our results still offer an insight into users who have varied technical backgrounds and specifically a comparison of users who showed some crypto-knowledge versus those who did not. According to a recent study on the external validity of surveys on privacy and security [31], Prolific users are significantly more knowledgeable about privacy and security matters than the overall U.S. population. Although we recruited people within the EU, the results of [31] suggest that our participants classified as laypersons may be much more knowledgeable than the overall EU population. Further, around 74% of our survey participants had undergraduate or graduate degrees. That said, although the functional description helped laypersons of our study to correctly answer on average half of the FE comprehension questions, the description still needs to be improved and simplified to meet the needs of users who belong to the 'lay' spectrum of the overall EU population.

6 CONCLUSIONS

Our studies have investigated the usability of two explanations (functional and structural) of functional encryption for helping people make informed decisions. We investigated a data-sharing scenario with studies targeting both experts and laypersons using a mixed-method approach. Our studies' participants who are interested in privacy explanations show clear preference and satisfaction criteria, as well as varied comprehensions of the provided explanations. Results relating to expert participants seem to be similar to lay participants, apart from preferring the structural explanation. Overall when compared, participants are more satisfied with the structural explanation. However, the comprehension of participants exposed to the functional explanation was significantly better than the ones exposed to the structural one. Although there is a discrepancy between preference, satisfaction, and comprehension of the descriptions, participants who are interested in the descriptions seem to appreciate one or the other to some degree nevertheless. To conclude, our results indicate that each description fulfills a different need and that offering both types of explanations is useful for users' preferences, satisfaction, and correct comprehension. We specifically recommend combining both descriptions in multi-layered policy notices.

ACKNOWLEDGMENTS

This work was funded by the H2020 Framework of the European Commission under Grant Agreement No. 786767 (PAPAYA project) and by the Swedish Knowledge Foundation (TRUEdig project). The work was also supported by the Wallenberg AI, Autonomous Systems and Software Program (WASP) funded by the Knut and Alice Wallenberg Foundation. The authors acknowledge John Sören Pettersson for his contribution to Study A's design and discussions, Elin Nilsson for her help with Study A's interactive mock-ups, transcriptions, and walk-throughs, Sébastien Canard and Melek Önen for providing the use-case, technical advise and recruiting participants for Study A, and Matthias Beckerle for his contribution in form of a first version of a FE structural explanation mock-up as well as to Study B's early discussions. We extend our thanks to all the study participants who volunteered and contributed to this research as well as the anonymous reviewers for their helpful feedback.

REFERENCES

[1] Ruba Abu-Salma, Elissa M. Redmiles, Blase Ur, and Miranda Wei. 2018. Exploring User Mental Models of End-to-End Encrypted Communication Tools. In *8th USENIX Workshop on Free and Open Communications on the Internet (FOCI 18)*. USENIX Association, Baltimore, MD, 8 pages.

[2] Omer Akgul, Ruba Abu-Salma, Wei Bai, Elissa M. Redmiles, Michelle L. Mazurek, and Blase Ur. 2021. From Secure to Military-Grade: Exploring the Effect of App Descriptions on User Perceptions of Secure Messaging. In *WPES '21: 20th ACM Workshop on Privacy in the Electronic Society* (Virtual Event, Republic of Korea) *(WPES '21)*. Association for Computing Machinery, New York, NY, USA, 119–135. https://doi.org/10.1145/3463676.3485602

[3] Omer Akgul, Wei Bai, Shruti Das, and Michelle L Mazurek. 2021. Evaluating {In-Workflow} Messages for Improving Mental Models of {End-to-End} Encryption. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, Berkeley, 447–464.

[4] Ala Sarah Alaqra, Simone Fischer-Hübner, and Erik Framner. 2018. Enhancing privacy controls for patients via a selective authentic electronic health record exchange service: qualitative study of perspectives by medical professionals and patients. *Journal of medical Internet research* 20, 12 (2018), e10954.

[5] Ala Sarah Alaqra, Bridget Kane, and Simone Fischer-Hübner. 2021. Machine Learning–Based Analysis of Encrypted Medical Data in the Cloud: Qualitative Study of Expert Stakeholders' Perspectives. *JMIR human factors* 8, 3 (2021), e21810.

[6] Maria Bada, Angela M Sasse, and Jason RC Nurse. 2019. Cyber security awareness campaigns: Why do they fail to change behaviour? , 11 pages. arXiv:arXiv:1901.02672

[7] Wei Bai, Michael Pearson, Patrick Gage Kelley, and Michelle L Mazurek. 2020. Improving non-experts' understanding of end-to-end encryption: An exploratory study. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, New York, 210–219.

[8] Matthias Beckerle, Simone Fischer-Hubner, Nuria Ituarte, Jonathan Magnusson, Patrick Murmann, Angel Palomares Perez, Tobias Pulls, John Soren Pettersson, Jonas Frei, and Christian Weis. 2020. PAPAYA Deliverable D3. 4– Transparent Privacy Preserving Data Analytics. https://www.papaya-project.eu/sites/default/files/papaya/public/content-files/deliverables/PAPAYA_Deliverable_D3_4.pdf

[9] Veroniek Binkhorst, Tobias Fiebig, Katharina Krombholz, and Wolter Pieters. 2022. Security at the End of the Tunnel: The Anatomy of VPN Mental Models Among Experts and Non-Experts in a Corporate Context. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Boston, MA, 3433–3450.

[10] Dan Boneh, Amit Sahai, and Brent Waters. 2011. Functional encryption: Definitions and challenges. In *Theory of Cryptography Conference*. Springer, Berlin, Heidelberg, 253–273.

[11] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.

[12] Jean Camp, Farzaneh Asgharpour, Debin Liu, and IN Bloomington. 2007. Experimental evaluations of expert and non-expert computer users' mental models of security risks. , 24 pages.

[13] Sébastien Canard, Ala Sarah Alaqra, Jérémy Chotard, Simone Fischer-Hübner, Bridget Kane, Stéphane Guilloteau, Dominique Le Hello, Elin Nilsson (KAU), John Sören Pettersson, and Bastien Vialla. 2021. PAPAYA Deliverable D5.2 – TELECOM USE CASE VALIDATION. https://www.papaya-project.eu/sites/default/files/papaya/public/content-files/deliverables/PAPAYA_D5.2_Telecom_Use_Case_Validation_final.pdf

[14] Albese Demjaha, Jonathan M Spring, Ingolf Becker, Simon Parkin, and M Angela Sasse. 2018. Metaphors considered harmful? An exploratory study of the effectiveness of functional metaphors for end-to-end encryption. In *Proc. USEC*, Vol. 2018. Internet Society, United States, 1–11.

[15] Andrea A. diSessa. 19895. Models of computation. In *User Centered System Design: New Perspectives on Human-Computer Interaction*, D. A. Norman and S. W. Draper (Eds.). Lawrence Erlbaum Associates, Hillsdale, New Jersey.

[16] Verena Distler, Carine Lallemand, and Vincent Koenig. 2020. Making Encryption Feel Secure: Investigating how Descriptions of Encryption Impact Perceived Security. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, New York, 220–229. https://doi.org/10.1109/EuroSPW51379.2020.00037

[17] EU-GDPR. 2022. Article 7 EU General Data Protection Regulation. Conditions for consent. https://www.privacy-regulation.eu/en/article-7-conditions-for-consent-GDPR.htm

[18] Kevin Gallagher, Sameer Patil, and Nasir Memon. 2017. New Me: Understanding Expert and Non-Expert Perceptions and Usage of the Tor Anonymity Network. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, 385–398.

[19] Katherine Hamilton, Shin-I Shih, and Susan Mohammed. 2016. The development and validation of the rational and intuitive decision styles scale. *Journal of personality assessment* 98, 5 (2016), 523–535.

[20] Milena Janic, Jan Pieter Wijbenga, and Thijs Veugen. 2013. Transparency enhancing tools (TETs): an overview. In *2013 Third Workshop on Socio-Technical Aspects in Security and Trust*. IEEE, New York, 18–25.

[21] Rohit Khare. 2022. Privacy Theater: Why Social Networks Only Pretend To Protect You. https://techcrunch.com/2009/12/27/privacy-theater/

[22] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel von Zezschwitz. 2019. "If HTTPS Were Secure, I Wouldn't Need 2FA" - End User and Administrator Mental Models of HTTPS. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, New York, 246–263. https://doi.org/10.1109/SP.2019.00060

[23] Ada Lerner, Eric Zeng, and Franziska Roesner. 2017. Confidante: Usable Encrypted Email: A Case Study with Lawyers and Journalists. In *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, New York, 385–400. https://doi.org/10.1109/EuroSP.2017.41

[24] Alexander De Luca, Sauvik Das, Martin Ortlieb, Iulia Ion, and Ben Laurie. 2016. Expert and Non-Expert Attitudes towards (Secure) Instant Messaging. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 147–157.

[25] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research* 15, 4 (2004), 336–355.

[26] MentimeterAB. 2022. Interactive presentation software - Mentimeter. https://www.mentimeter.com/

[27] Prolific. 2022. Quickly find research participants you can trust. https://www.prolific.co/

[28] Erica Racine, Patrick Skeba, Eric PS Baumer, and Andrea Forte. 2020. What are PETs for Privacy Experts and Non-experts. In *Symposium on Usable Privacy and Security*. USENIX Association, Berkeley, 6 pages.

[29] Leonie Schaewitz, David Lakotta, M. Angela Sasse, and Nikol Rummel. 2021. Peeking Into the Black Box: Towards Understanding User Understanding of E2EE. In *Proceedings of the 2021 European Symposium on Usable Security* (Karlsruhe, Germany) *(EuroUSEC '21)*. Association for Computing Machinery, New York, NY, USA, 129–140. https://doi.org/10.1145/3481357.3481521

[30] Mary Anne Smart, Dhruv Sood, and Kristen Vaccaro. 2022. Understanding Risks of Privacy Theater with Differential Privacy. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW2, Article 342 (nov 2022), 24 pages. https://doi.org/10.1145/3555762

[31] Jenny Tang, Eleanor Birrell, and Ada Lerner. 2022. Replication: How Well Do My Results Generalize Now? The External Validity of Online Privacy and Security Surveys. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. USENIX Association, Berkeley, 367–385.

[32] Justin Wu and Daniel Zappala. 2018. When is a Tree Really a Truck? Exploring Mental Models of Encryption. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Baltimore, MD, 395–409.

[33] Yixin Zou, Abraham H Mhaidli, Austin McCall, and Florian Schaub. 2018. " I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Berkeley, 197–216.

A STUDY GUIDE

Pre-study correspondence We send out invitation letters containing the objective and description of the study. We also include the consent forms beforehand.

Introductions. Welcome and introduction of the study, agenda, study set-up, and protocol. (breakout rooms open for UI mock-up walk-throughs as they are run in parallel)

A.1 Protocol of UI mock-ups walk-throughs

(1) We welcome the respondent and introduce the study and setup: zoom, UI mock-ups, and agenda of the study.
(2) Purpose"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. We are interested in your opinions/perspectives; there are no right or wrong answers so feel free to express yourself in this study. All responses are voluntary."
(3) We present the use case: "In this study, we have a use case, where a Telecom provider called TelecomAB, offers a service in their application. In this service, app users are asked if they would participate and contribute their personal user data for a statistical survey. The data should be protected by PAPAYA's Privacy by Design approach".
(4) We present the task of walk-through the mock-ups and the non-interference of the moderator
(5) Instructions prior to screen sharing for privacy reasons
(6) Consent is given prior to the recording of the session
(7) walk-through begins: the respondent goes through the mock-ups and the moderator observes and takes notes of parts clicked on
(8) post-walk-through questionnaire
    - Why did you not click on (a, b, c, d, e)? (a. More on TeleComAB's Privacy Impact Assessment and Privacy by Design approach b. How does it work? c. How are Privacy Risks reduced by our Privacy by design approach d. Clicks on more of any privacy risk e.g. 1: "Illegitimate Data Access (more)" e. Clicks on more of any privacy risks e.g., 2: "Linkable Data Processing potentially Identifying Users (more)")
    - Was there anything that was unclear (a, b, c, d, e)?

(a short break and re-collection at zoom main room for focus groups session)

A.2 Focus groups workshop

Setup. Technical introductions and preparations of zoom and Mentimeter, some pilot testing of a few unrelated questions prior to starting the discussion.
Incentives questions. S1: Would you generally contribute to participating your data in this UC? (yes/no) S2: Would you consent to participating your data if offered a discount on your subscription or in this case, an Amazon voucher? S3: What offers/incentives would motivate you to consent? (you can submit multiple times: 2 minutes)
Discussion of the incentives. " Which of the following incentives do you agree to? We now go around starting with…" (based on the inputs by participants, which facilitated the discussion) (go-arounds: participants talked one by one) "Which of the following incentives you do not agree to? We now go around starting with…" (go-arounds)

S4: "Which of the following do you consider a benefit to you to share your data: you rank the options from 1st, most significant, to 4th: Sustainability and environmental purposes, City planning and public transport, Tracking of COVID-19 cases, Discounts and Vouchers"
Descriptions and mental models. S5: "Which of the following terms do you think is most suitable for mediating (to different types of users) That TelecomAB cannot read/access the user data in 'clear text'. The information is first 'summarized' then concealed by altering it so that it appears to be random data, e.g. 'Password' is concealed as '&t#dFF01': "Aggregated and securely encoded data" "Aggregated and securely encrypted data" "Aggregated and securely protected data"

S6: What alternative descriptions do you think are suitable? Now we go around and discuss why: "Aggregated and securely encoded data" is suitable/not suitable?" (go-arounds) "Aggregated and securely encrypted data" is suitable/not suitable?" (go-arounds) "Aggregated and securely protected data" is suitable/not suitable?" (go-arounds) "can you think of alternative descriptions?- keep in mind the general public: different types of users" (go-arounds) Functionality: we share the link to the mock-ups again ——5 minutes break—– "See the following description of privacy functionality: S7: '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.' What are your thoughts on the description? Is the explanation well understood? Is there anything missing?" (go-arounds)

S8: "See the following description of functional encryption, What are your thoughts on the description? Is the explanation well understood? Is there anything missing?" (go-arounds)

S9: "Which description do you prefer?" Why and comments (go-arounds)

S10: "What are your thought on the presentation of the risks? What do you understand from the visualization? Is there anything missing? (go-arounds)
Questions on comprehension. S11: "from the data that the user contributes to the study, do you think that TeleComAB can directly see the user's social network usage information? Yes, no, not sure (give a few minutes to answer) We can go around and say why do you think so?" (go-arounds) [correct answer: No]

S12: Which data do you think is [securely encoded]:

- the data sent by the user to TelecomAB [correct answer]
- the statistical analysis result that TelecomAB produces
- both
- none

(a few minutes were given to answer, and then we had go-arounds and the discussion of answers) S13a: "Who do you think can de-code/decrypt/access the data that the user sends in clear text

- TelecomAB
- MediaSurvey Cooperation that requests the result
- both
- none [correct answer]

(a few minutes were given to answer, and then we had go-arounds and the discussion of answers) – we show the description

again then repeat the question ‘S13b’, then discussion again–

Questionnaire. The respondent is asked to fill out the demographics questionnaire and then thanked for their participation.

A.3 FE explanations in study A

Figure 3 shows the functional explanation offered to participants in focus group workshops and Figure 4 shows the structural description.

A.4 Expertise detailed demographics

Table 2 shows the participants’ demographics in our focus groups (Study A).

A.5 CODEBOOK WITH OVERALL THEMES

Table 3 shows the overall codes under the main and sub-themes of study A.

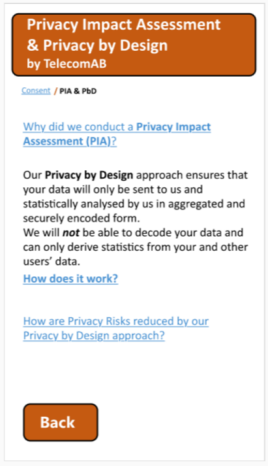
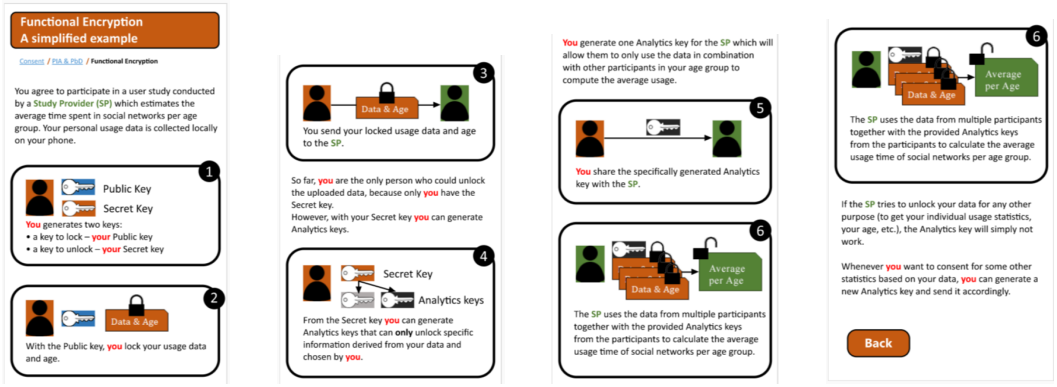


Figure 3: Functional description of FE in Study A.



(a) First screen - The first two steps

(b) Steps three and four.

(c) Steps five and six.

(d) The last screen.

Figure 4: Structural explanation of FE in study A - (a): the first screen describing the first two steps, (b)(c)(d): the upcoming steps appearing as the user scrolls down.

Participant	FG	Expert	Gender	Exp. CS	Exp. DA	Exp. FE	Exp. cryptography
p1	FG0	no	Female	Proficient	Adv. beginner	Novice	Novice
p2	FG0	no	Male	Inexpert	Inexpert	Inexpert	Inexpert
p3	FG0	no	Male	Adv. beginner	Adv. beginner	Novice	Novice
p4	FG1	yes	Female	Adv. beginner	Novice	Adv. beginner	Competent
p5	FG1	yes	Male	Proficient	Novice	Novice	Competent
p6	FG1	yes	Male	Adv. beginner	Inexpert	Novice	Proficient
p7	FG2	no	Female	Adv. beginner	Novice	Inexpert	Inexpert
p8	FG2	no	pnts	Inexpert	Competent	Inexpert	Inexpert
p9	FG2	no	Female	Competent	Inexpert	Inexpert	Inexpert
p10	FG2	no	Female	Inexpert	Inexpert	Inexpert	Inexpert
p11	FG3	yes	Male	Competent	Novice	Novice	Expert
p12	FG3	yes	pnts	Expert	Expert	Novice	Expert
p13	FG3	yes	Male	Expert	Competent	Expert	Expert

Table 2: Overview of study A participants, demographics, and expertise in computer science (CS), data aggregation (DA), functional encryption (FE), and cryptography

Table 3: Themes, subthemes, and corresponding codes per focus group and participant

Theme and sub-themes	Code (instances)	Focus group	References
1. Incentives and data sharing			
1.1 Factors hindering sharing (10)		FG1, FG2, FG3	p4-p13
	Concerns about the incentive Provider (2)	FG2	p8,p10
	Habit to not share (6)	FG1, FG2, FG3	p5,p6,p8,p9, p12, p13
	Negative experience affecting trust (2)	FG2	p7,p10
	Unappealing monetary incentive (7)	FG1, FG2, FG3	p4,p5,p8,p9,p11,p12,p13
	Negative impression of sharing for money (4)	FG1, FG3	p5,p6,p11,p12
	Data Privacy concerns (5)	FG2,FG3	p7,p8,p10,p12,p13
1.2 Factors motivating sharing (13)		FG0, FG1, FG2,FG3	p1-p13
	Monetary incentive as an added value (5)	FG0, FG1, FG2	p1,p4,p5,p6,p7
	Direct benefits to users (5)	FG1, FG3	p5,p6,p11,p12,p13
	Transparency, Privacy and security considerations (3)	FG1, FG2	p5,p7,p8
	Societal-common good (13)	FG0, FG1,FG2,FG3	p1-p13
	Sharing for common good only if Privacy is Preserved (3)	FG1, FG3	p5,p6,p12
	Clear and justifiable purpose of use (9)	FG0, FG1, FG2, FG3	p3,p4,p5,p6,p8,p9,p11,p12,p13
2. Perceptions of the addressed terminologies			
2.1 Opinions and preferences – encrypted (13)		FG0, FG1, FG2, FG3	
	Preferred encrypted for the general Public (2)	FG3	p12,p13
	Overall preference for encrypted (12)	FG0, FG1, FG2, FG3	p1-p11,p13
	Encrypted too specific and misleading (2)	FG3	p11,p13
	Encrypted Preferred Personally (12)	FG0, FG1, FG2, FG3	p1-p11,p13
	Term gives feeling of safe and secure (3)	FG0, FG3	p2,p3,p12
	Term gives professional feel (2)	FG2	p7,p9
	Widespread use of term (2)	FG3	p12,p13
	Term connection to IT knowledge (2)	FG0	p1,p3
2.2 Opinions and preferences – protected (10)		FG0, FG1, FG2	
	Preferred Protected for the general Public (5)	FG0, FG1	p1,p3,p4,p5,p6
	Sense of safety with term (2)	FG0	p1,p2
	Unclear meaning with term (4)	FG2	p7,p8,p9,p10
2.3 Opinions and preferences – encoded (8)		FG0, FG1, FG3	
	Lack of association with security or reassurances (7)	FG0, FG1, FG3	p1,p2,p3,p5,p6,p12,p13
	General meaning understandable (1)	FG3	p11
3. Descriptions preferences and feedback			
3.1 Structural description appreciated (10)		FG0, FG1, FG2, FG3	p2,p3,p4,p5,p6,p7,p8,p11,p12,p13

Theme and sub-themes	Code (instances)	Focus group	References
	Structural description preferred (9)	FG0, FG1, FG2, FG3	P2, P3, P4, P5, P6, P7, P11, P12, P13
	Appreciation of graphics and visual appeal (5)	FG0, FG1, FG3	P2, P3, P5, P6, P13
	Appreciation of step-by-step illustration (4)	FG0, FG1	P3, P4, P5, P6
	Appreciation of technical details on how it works (5)	FG1, FG2, FG3	P5, P6, P7, P11,P12
	Structural explanation leads to trust (3)	FG1, FG3	P4, P5, P12
	Structural explanation leads understanding (4)	FG0, FG1, FG3	P3, P4, P5, P12
3.2 Functional description preferred (4)		FG0, FG2	P1,P8,P9,P10
	Quicker to read (2)	FG0, FG2	P1, P9
	Sufficient information (3)	FG2	P8, P9,P10
3.3 Combination of both descriptions preferred (4)		FG0, FG2	P1, P7, P8, P10
4. Comprehensions of FE			
4.1 Understanding Telecom AB only gets encrypted user data			
	Correct answers with description reference (5)	FG0, FG1, FG2	P2, P3, P5, P6, P9
	Unsure about the answers (6)	FG0, FG1, FG2, FG3	P1, P4, P8, P10, P11, P13
	Anonymity set size reasoning for not sure (1)	FG1	P4
	Meta data reasoning for yes (1)	FG3	P12
	Re-identification risks concern for not sure (1)	FG0	P1
	Hacking risks concern for yes (1)	FG2	P7
4.2 Understanding only data sent is securely ‘encoded’			
	Correct answers (9)	FG0, FG1, FG2, FG3	P1, P2, P3, P4, P5, P7, P10, P11, P12, P13
	Unsure about correct answer (2)	FG1, FG2	P6, P9
	Security uncertainty (1)	FG2	P8
4.3 Understanding that others cannot decrypt user data (unchanged answers)			
	Correct answers (6)	FG1, FG2, FG3	P4, P5, P6, P9, P11, P12
	Answers based on structural description (3)	FG1, FG3	P5, P11, P12
	Misconception statistical analysis requires unencrypted data (3)	FG0, FG3	P1, P2, P13
	Misunderstanding the structural description (2)	FG0, FG2	P3, P7
	Encryption attacks risks (1)	FG2	P8

B SURVEY

After giving their consent, survey participants first answered demographic questions (see Section B.4). Then they were exposed to the data analysis scenario of our survey (presented in Section B.1), answered some related questions (pre-explanation decision-related questions in Section B.4), got exposed to either functional (presented in Section B.2) or structural description (presented in Section B.3), answered concerning questions (post-explanation decision-related questions followed by comprehension questions and questions on opinion and satisfaction in Section B.4), and finally completed the survey by answering two standardized questionnaires (privacy concern and decision-making style scales in Section B.4).

B.1 Data analysis scenario

In this scenario imagine that:

(1) You are a customer of a telecommunication company called TeleCom AB.
(2) You voluntarily download an app that belongs to TeleCom AB:
   - The app is a privacy-preserving smartphone usage analytics app.
   - If the app users consent, then:
     - In a privacy-friendly manner, the app collects and shares a selection of data from the user with TeleCom AB.
     - TeleCom AB would then produce statistics on users' usage of mobile apps based on requests from third parties.
(3) The app has notified you and other users about a new request from a third party called MediaSurvey Corporation:
   - The new request is for statistics about the average time users use social network apps per day depending on their age.
   - If you give consent to the request, you will receive a 5-euro voucher from TeleCom AB.
   - TeleCom AB will process your data (together with data provided by other users) and share the statistics with MediaSurvey Corporation in a privacy-friendly manner.

B.2 FE explanation - Functional

In the previous scenario, you were informed that your data will be collected, analyzed, and shared in a privacy-preserving process. The following is a description of how your privacy will be protected:

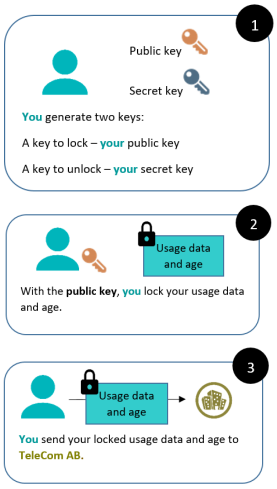
"Our (TeleCom AB's) privacy approach ensures that your data is aggregated and securely encrypted before being shared/sent to us, meaning that no personal information about you could leak to us. We statistically analyze your encrypted data together with data of other users to derive statistical results.

Your data that you share/send to us will always remain encrypted and no one will be able to decrypt your data even during the statistical analysis. However, data in form of the statistical results will be derived and shared with the third party (MediaSurvey Corporation) that requested the statistics. Both TeleCom AB and MediaSurvey Corporation can access the statistical results in plain text (in decrypted form)."

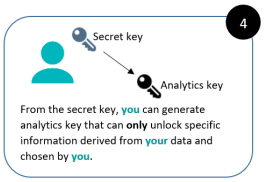
B.3 FE explanation - Structural

In the previous scenario, you were informed that your data will be collected, analyzed, and shared in a privacy-preserving manner. The following is a description of how your privacy will be protected:

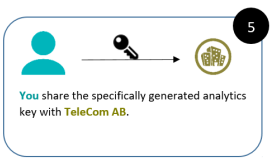
You agree to participate in a study conducted by TeleCom AB. The study is requested by a third party, MediaSurvey Corporation. The study has the purpose to estimate the average time spent on social networks per age group. Your personal usage data and age are collected locally on your phone. Then, the following steps are taken by you (or more precisely by your app), as well as other users and TeleCom AB:

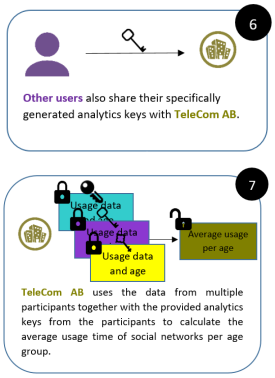


So far, you are the only person who could unlock the shared data, because only you have the secret key. However, with your secret key, you can generate an analytics key.



You generate one analytics key for TeleCom AB that will only allow them to use the data in combination with other participants in your age group to compute the average time of using social network apps.





TeleCom AB shares the statistical results with the third-party MediaSurvey Corporation which requested the statistics.

If TeleCom AB tries to unlock your data for any other purposes (to get your individual usage statistics, your age, etc.) the analytics key will simply not work.

Whenever you want to consent to some other statistics based on your data, you can generate a new analytics key and send it accordingly.

B.4 Overview of Survey Questions

Demographics:

(1) What is your age? (Options: 18-24, 25-39, 40-65, 66+, prefer not to say (pnts))
(2) What gender do you identify as? (Options: Female, Male, Other, pnts)
(3) Which of these is the highest level of education you have completed? (Options: No formal qualifications, Secondary education, High school diploma/A-levels, Technical/community college, Undergraduate degree, Graduate degree)
(4) What is your subject of study? (We provided a list of subjects based on the same question on the Prolific website)

[After demographics, participants were instructed to read the scenario (see Section B.1)]

Pre-explanation decision-related questions:

(1) Would you give your consent to the request in the scenario above (if you were exposed to it)? (Options: No, Yes, It depends, Unsure/I do not know)
(2) (If the answer was "Yes" on the first question:) Which of the following is a reason for your decision to give consent (select all that apply)? (Options: I would not mind giving my consent for sharing my data in general, I would like to receive the 5 euro voucher, I trust TeleCom AB with my data, I would like to contribute to better results of data analytics, Other [text field])
(3) (If the answer was "No" on the first question:) Which of the following is a reason for your decision to NOT give consent (select all that apply)? (Options: I usually do not give my consent for sharing my data in general, I generally worry about the privacy and security of my data, I have doubts about TeleCom AB, I have doubts about the third party MediaSurvey Corporation, The 5 euro voucher that is offered in exchange of my data, The purpose of statistics is unclear, Other [text field])
(4) (If the answer was neither "Yes" nor "No" on the first question:) Which of the following is a reason for your answer (select all that apply)? (Options: I have doubts about TeleCom AB, I have doubts about MediaSurvey Corporation, The 5 euro voucher that is offered in exchange for my data, I have doubts about the privacy and security of my data, The purpose of statistics is unclear, Other [text field])
(5) Which of the following purposes would you consider a benefit to share your data in this scenario (select all that apply)? (Options: If my data is used to benefit of society (such as city planning based on the statistical results), If I receive a sufficient monetary incentive (such as discounts and vouchers), If my data is used for research purposes, If the results of the study are published or made accessible, If my data is used to improve services and products that I use, Other [text field])

Post-explanation decision-related questions:

(1) Now that you know more about data processes in the scenario we repeat the last question: Would you give your consent to the request in the scenario previously described? (Options: No, Yes, It depends, I am not sure/ I do not know)
(2) (If the answer was "Yes" on the first question:) Why would you give consent? [Open text field]
(3) (If the answer was "No" on the first question:) Why would you NOT give consent?
(4) (If the answer was neither "Yes" nor "No" on the first question:) What made you unsure about giving your consent?
(5) (If they answered differently compared to their answer to the first question in B.4:) Why did you change your previous decision about giving consent?

Comprehension questions:

(1) Who do you think can decrypt the data that the user (i.e. you) sent? (Options: TeleCom AB, MediaSurvey Corporation that requests the result, Both, None, I do not know/not sure)
(2) Which data do you think is encrypted? (Options: The data sent by users to TeleCom AB, The statistical results that TeleCom AB produces, Both, None, I do not know/not sure)
(3) Can TeleCom AB access the results of the statistical analysis in plain text (non-encrypted form)? (Options: Yes, No, I am not sure/I do not know)
(4) Can MediaSurvey Corporation access your results of statistical analysis in plain text (i.e. in non-encrypted form)? (Options: Yes, No, I am not sure/I do not know)

Questions on opinion and satisfaction:

(1) Do you agree or disagree with the following statements? (Five-point Likert scale options)
- I am satisfied with the level of detail in the description
- I am satisfied with the presentation of the description
- I am satisfied with the length of the description
- I am satisfied with the wording/terminology used in the description

(2) I found the explanation of how my privacy is protected ... (Five-point Likert scale options)
- Understandable

- Convincing
- Trustworthy
- Easy to read

(3) Do you agree or disagree with the following statement? (Five-point Likert scale options)
- The description helps me make informed consent about sharing my data in the scenario.

Privacy concern and decision making style scales: We used global information privacy concern scale items from [25] and rational and intuitive decision style scale items from [19].