New Differential Privacy Communication Pipeline and Design Framework

Jingyu Jia
Nankai University

Zikai Alex Wen*
HKUST(GZ)

Zheli Liu
Nankai University

Changyu Dong*
Guangzhou University

Abstract

Organizations started to adopt differential privacy (DP) techniques hoping to persuade more users to share personal data with them. However, most users do not understand DP techniques, thus still not willing to share. Previous research suggested that the design of DP mechanism communication could influence users' willingness to share data. Based on the results of prior work, we propose a new communication pipeline that starts with asking users about their privacy concerns and then provides customized DP mechanism and communication. We also propose a design framework that can systemically explore effective communication designs ranging from a text-based high-level description to a step-by-step interactive storyboard. Based on the framework, we created 17 designs and recruited 5 people to evaluate and to co-design. Our co-design study showed that text-based descriptions have the highest clarity in all scenarios, while the step-by-step interactive storyboards have potential in persuading users to trust *central DP*. Our future work will optimize the DP communication designs and conduct a large-scale efficacy study.

1 Introduction

Organizations have been striving hard to persuade users to share personal data with them. To achieve this goal, the organizations must use privacy-preserving technologies to prevent users' sensitive data from being leaked. In addition, they need to convince their users to trust that their technologies can indeed protect users' privacy, so that the users will be willing to share data. That being said, many technologies are available for data protection. To identify what privacy-preserving technology is suitable for a particular occasion, there are needs for proofing and comparing the data protection efficacy of different technologies. To meet the needs, security and privacy researchers [2, 4–6] have been working on a technique called differential privacy (DP).

*Zikai Alex Wen and Changyu Dong are the corresponding authors.

Table 1: Seven Types of Privacy Concerns

No.	Abbreviation	Description
1	Hack	My data will be hacked by hackers.
2	Law	My data will be forcibly acquired by the government.
3	Organization	My data will be stolen by unrelated employees in the organization.
4	Disclosure	My data will be disclosed to others by the organization.
5	Analyst	My data will be accessed by the data analysts in the organization.
6	Graphs	The graphs and tables generated by the organization will reveal my data.
7	Share	The organization will reveal my data when sharing the processed dataset with others.

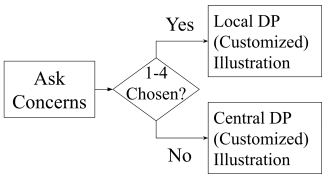

Figure 1: The communication pipeline asks about the user's privacy concerns to match customized DP and illustration.

DP evaluates the efficacy of a privacy-preserving technology by quantifying the difference between two data analysis results that are processed by the technology. These two analysis results are calculated from two datasets: one dataset that collects the individual user's data and another dataset that does not collect the data. If the aforementioned results are not significantly different, then the privacy-preserving technology is proved to satisfy the DP mechanism. In this case, it is unlikely to identify an individual user's record through queries protected by a DP mechanism.

However, it is difficult for ordinary users to understand the proof of DP. Therefore, the organizations also need to persuade users that using DP can prevent their personal data from being leaked. Currently, most organizations rely on text-based descriptions to communicate the DP mechanism with

users (e.g., Apple's white paper [1]). In addition, it is still debatable whether the existing DP communication designs, including text-based [3] and animation-style [12] designs, may persuade more users to share their data.

Therefore, our work takes a step further to seek effective ways to communicate DP mechanisms with ordinary users. First, we combined key takeaways from prior work [3, 12] to design a new communication pipeline (as shown in Figure 1) that attempts to address different types of user concerns. Second, we proposed a communication design framework that consists of four categories: (1) text-based description, (2) data input/output illustration, (3) data output probability distribution illustration, and (4) step-by-step interactive storyboard illustration.

To study what communication design would be clear and persuasive, guided by the framework, we created nine designs to persuade users into sharing *numerical* salary data and eight designs to persuade users into sharing *geographical* location data (as shown in Figure 2). After that, we conducted a one-on-one co-design study with four ordinary users and one DP researcher to evaluate the 17 designs and provide feedback about narrowing the designs down to the effective ones. We list and discuss our key findings in the co-design study section.

2 Related Work

Recently, an increasing number of research projects have studied how to help users understand DP mechanism and to persuade users to share their data [3, 7–9, 11, 12]. Xiong et al. [11, 12] investigated how textual and illustration descriptions of DP affect users' understanding of DP and willingness to share data. They found that providing respondents with DP descriptions facilitated data sharing and that illustrations effectively describe DP models to users. Nanayakkara et al. [9] designed an interactive visualization tool for data managers with experience in sensitive data analysis but unfamiliar with DP to help them effectively set DP parameters.

Franzen et al. [7] explained DP to users through a risk communication format, and they found that emphasizing DP risks rather than DP functionality, while not affecting users' objective understanding of DP, can reduce subjective confidence in their understanding. Cummings et al. [3] found that in-the-wild DP descriptions do not match users' privacy concerns and do not promote data sharing. They proposed that solutions matching users' privacy concerns better promote users' data sharing. Combined with prior works, our goal is to design an interactive illustration descriptions framework that can match users' privacy concerns and thus facilitate data sharing.

3 New Pipeline and Design Framework

This work aims to find effective ways to persuade more users to share their data if they realize that the data is protected by a DP technique. We deduced from prior research [3] that users would prefer a customized privacy notification to address their specific concerns. Therefore, we propose to change the traditional "read-then-consent" approach to inform users the privacy policy. We designed a new communication pipeline that starts with asking users their privacy concerns then provides the suitable DP technique and a customized privacy notification. Our work focuses on designing a critical part of the privacy notification: a clear and persuasive DP technique explanation. To systemically study what designs meet our goal, we propose a framework that covers four design categories ranging from non-interactive high-level description to interactive storyboard illustration.

In this section, we first describe the design of our DP communication pipeline and explain the rationale behind the design. Then, we describe the framework for designing the DP information. Following this, we describe how we followed the design framework to create nine designs to persuade users to share salary data and eight designs for sharing location data.

Communication Pipeline. As shown in Figure 1, the communication pipeline starts from presenting seven major data privacy concerns to the user then asks the user to choose the concerns that they have. The definition of seven privacy concerns (as shown in Table 1) is adapted from Cumming et al.'s definition [3]. We added *Disclosure* to the original definition to provide finer granularity, which allows the system to identify the level of trust between the user and the organization.

If it concerns the user that the organization may disclose raw user data without their additional consent then they should choose *Disclosure*. But if the user trusts the organization to share privacy-preserving data with others and only have concern about the reliability of the privacy-preserving technique, then they can choose *Share*. We also refined the description of *Organization* so that if the user worries about unauthorized data access inside the organization then they should choose it. If the user worries about authorized data access inside the organization, then they can choose *Analyst*.

After the system receives the user's response, it decides which level of DP, *local DP* or *central DP*, can address the user's concerns. Then the system explains to the user how the DP mechanism would resolve their concerns before it asks for consent. According to our analysis, if the user chooses one of the concerns from No.1 to No.4, then they need the strict DP mechanism: *local DP*. *Local DP* requires the system to add noise to the user's data on the user's local computing platform before it uploads the data to its cloud storage. In comparison, if the user only chooses the concerns from No.5 to No.7, then the system can use a less strict DP mechanism: *central DP* because the user indicates that they trust the organization to protect their privacy. By using *central DP*, the organization can store users' raw data and only adds noise to the original data when sharing it with authorized employees or other parties to preserve users' privacy.

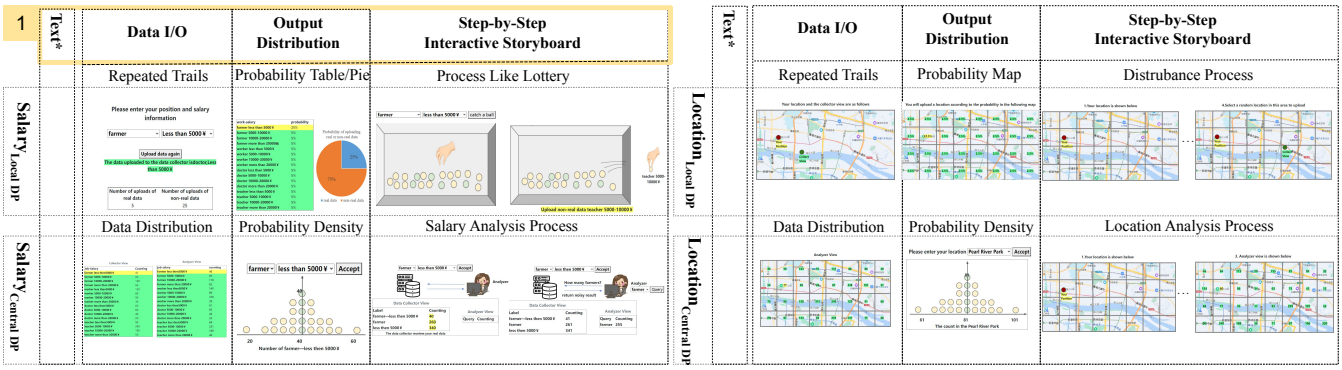

Figure 2: This diagram shows our design framework of four design categories. *Highlight 1* shows the four design categories. It also shows nine designs for salary data request scenario and eight designs for location data request scenario. *Text** is the category of all text-based descriptions for four design scenarios: *local DP* and *central DP* for salary data protection and *local DP* and *central DP* for location data protection.

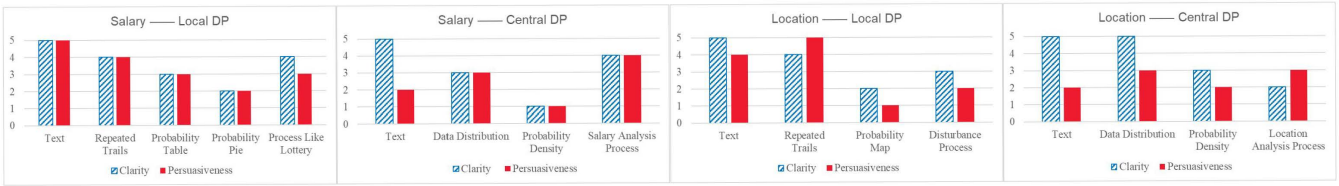

Figure 3: The histograms show the number of participants agreed or strongly agreed that a design is clear or persuasive.

Design Framework. Now that we have the ability to understand a user's specific privacy concerns through the communication pipeline, our next job is to design a customizable DP mechanism explanation that can allay different types of user concerns. To systemically study possible effective designs, we propose a framework that consists of four design categories (as shown in Figure 2, Highlight 1): (1) text-based description, (2) data input/output illustration, (3) data output probability distribution illustration, and (4) step-by-step interactive storyboard illustration.

We created this framework to cover a spectrum of design categories: Category (1) provides a high-level description of a DP mechanism; Categories (2) and (3) provides pictorial illustrations about data output values or probability distributions; and Category (4) is a new type of design that we would like to explore: designing storyboards to explain a DP mechanism and using step-by-step interactions to scaffold the understanding. The design complexities increase from categories (1) to (4), but we suspect that a design is more user-friendly if it is contextualized and provides step-by-step interactive scaffolding.

To validate our hypothesis, based on the design framework, we created 17 designs for two data sharing request scenarios: nine designs for requesting salary data and eight designs for location data. Previous work [3, 12] designed communication methods for these two scenarios respectively. Cumming et al.'s design [3] falls into category (1) and Xiong et al.'s design [12] belongs to category (2-3) and the non-interactive version of (4). The following paragraphs describe the details of all 17 designs in a 4x4 design space: four design categories times four types of DP protected data sharing scenarios (i.e., protect salary data using *local DP* or *central DP* and protect location data using *local DP* or *central DP*).

(1) Text-Based Description: We followed the design of text-based description by Cummings et al. [3] to cover three pieces of DP information: (1) the specific data to be collected, (2) the timing to disturb the collected data, and (3) the explanation about why the party that concerns the user cannot infer personal data. We designed a text-based description template for each DP protected data sharing scenarios. The template includes seven sentences that aims to allay the seven privacy concerns respectively. These sentences can be formed into one paragraph if needed. Due to the page limited, we posted the templates document online [1]. We treat this design category as a design baseline because mainstream organizations (e.g., Apple [1]) are using this approach to explain the DP mechanism to their target users.

(2) Data Input/Output Illustration: As shown in Figure 2, we designed two *Repeated Trails* to illustrate the output processed by *local DP* and two *Data Distribution* for *central DP*. After the user enters an example data input, *Repeated Trails* shows the data output that the organization obtains. By repeatedly providing an example input, users may understand that the data output keeps changing under a certain rule so it may

[1] https://github.com/confide123/NDPCP/blob/main/7%20privacy%20concerns.docx

protect their privacy. *Data Distribution* illustrations showcase what data output the organization can produce for data queries. Users may understand that their individual records are accumulated. And even the accumulated dataset does not reflect the true user inputs. These designs illustrate data outputs, but they do not illustrate how the outputs are produced.

(3) Data Output Probability Distribution Illustration: We adapted Nanayakkara et al.'s design of discrete visualization of the statistical density graph [9] to create *Probability Density* illustrations. We followed their design because the design could help ordinary data managers understand the distribution of DP protected data. Managers can calculate the proportion of balls to the left of the output value to learn the probability of getting such an output value. We also followed the traditional practice to design *Probability Table and Pie Chart* and *Probability Map* to illustrate the mechanism of *local DP*. We suspect that these designs may require users to have knowledge about probability and statistics to comprehend.

(4) Step-by-Step Interactive Storyboard Illustration: The illustrations in this category may look various. However, we created them following certain guidelines. To illustrate how *local DP* functions, we designed storyboards that animate how the data input is disturbed on the local computing platform before it is obtained by the organization. To illustrate how *central DP* functions, we designed storyboards that first animate how the input data is obtained by the organization without any disturbance, then animate what the data queries can be, and finally animate how the organization adds noise to the data before it answers the data query. We suppose the storyboard can provide context and the step-by-step interactions provide mind breaks, which may make users feel more intuitive and easy to follow.

4 One-on-One Co-Design Study

To verify what DP communication designs are clear to ordinary users, and more importantly, can persuade users to share their data under DP protection, we conducted a one-on-one co-design study with five people.

Participants. We recruited five participants (4 ordinary users and 1 DP expert) through email and social media. The ordinary users' ages ranged from 19 to 57 years old. Two of them got high school degrees and the other two got bachelor degrees. The DP expert is 31-year-old and got a Ph.D. degree. They had between 9 and 30+ years of experience in using Internet. All of them experienced privacy breach and encounter bad consequences including harassment and/or receiving spam or phishing messages.

Procedure. The participant started by learning about DP knowledge from us to ensure that they have sufficient background knowledge to evaluate the designs and express their thoughts during the co-design session. This learning process is not included in the final communication design. After the participant finished learning, we asked them to experience the privacy communication pipeline and designs on our crafted websites: One is an income justice study survey and the other is a restaurant recommendation system. During co-design, the participant was asked to answer two five-point likert-scale questions for each design: (1) This design clearly describes the differential privacy mechanism; and (2) This design resolves my concern(s) so I feel comfortable to share my data. We followed up on the participant's evaluation and prompted them to refine the design if they have any thoughts. The entire study took about one and a half hours.

Method. We conducted the study face-to-face or remotely over Zoom. Participants received $30 cash. All co-design sessions were audio and screen recorded then transcribed. We used an open-coding technique [10] to find common themes shared across the co-design participants. In the key findings, we include quotes from participants identified by ID numbers following the letter P for "participant" (e.g. P1).

Key Findings and Discussion. All participants agreed or strongly agreed that text-based descriptions are clear under all conditions. That being said, **text-based description may not be the best approach to explain a *central DP* mechanism**. While all participants agreed or strongly agreed that texts were clear, only two participants were persuaded to share data. Let us take the location data request scenario for instance. Among them, P5 said she was willing to share even if the description is not clear because she had been sharing her location data all the time. In contrast, P2 was extremely cautious about sharing her location information because she had a terrible harassment experience after her location information was leaked. So, she rated the persuasiveness of all designs for *central DP* $\leqslant 3$. The rest three participants depend on the quality of communication material to decide whether they share location data. Text description was the least persuasive to them, while step-by-step storyboard illustrations showed potential in increasing the persuasiveness as long as it was clear to the user. P4 suggested that the text description was clear about how *central DP* mechanism can resolve his No. 7 concern, but he was skeptical until he could contextualize how his input became a privacy-preserving output as he interacted with the storyboard. So, our next design is to **combine text description with step-by-step interactive storyboard illustration**.

5 Conclusion and Future Work

In summary, we propose an new communication pipeline to first ask about the user's privacy concerns before providing a privacy notification. When it comes to designing the privacy notification, we propose to present a customized text-based description combined with a step-by-step interactive storyboard to illustrate how the DP mechanism may resolve concerns. We will implement it and conduct an "in-the-wild" experiment to test the efficacy of our proposed design.

References

[1] Apple differential privacy team Apple. Apple differential privacy technical overview. https://www.apple.com/privacy/docs/Differential_Privacy_Overview.pdf, 2017.

[2] Andrea Bittau, Úlfar Erlingsson, Petros Maniatis, Ilya Mironov, Ananth Raghunathan, David Lie, Mitch Rudominer, Ushasree Kode, Julien Tinnes, and Bernhard Seefeld. Prochlo: Strong privacy for analytics in the crowd. In *Proceedings of the 26th Symposium on Operating Systems Principles*, pages 441–459, 2017.

[3] Rachel Cummings, Gabriel Kaptchuk, and Elissa M Redmiles. " i need a better description": An investigation into user expectations for differential privacy. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pages 3037–3052, 2021.

[4] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating noise to sensitivity in private data analysis. In *Theory of cryptography conference*, pages 265–284. Springer, 2006.

[5] Cynthia Dwork, Aaron Roth, et al. The algorithmic foundations of differential privacy. *Found. Trends Theor. Comput. Sci.*, 9(3-4):211–407, 2014.

[6] Úlfar Erlingsson, Vasyl Pihur, and Aleksandra Korolova. Rappor: Randomized aggregatable privacy-preserving ordinal response. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*, pages 1054–1067, 2014.

[7] Daniel Franzen, Saskia Nuñez von Voigt, Peter Sörries, Florian Tschorsch, and Claudia Müller-Birn. " am i private and if so, how many?"–using risk communication formats for making differential privacy understandable. *arXiv preprint arXiv:2204.04061*, 2022.

[8] Farzaneh Karegar and Simone Fischer-Hübner. Vision: A noisy picture or a picker wheel to spin? exploring suitable metaphors for differentially private data analyses. In *European Symposium on Usable Security 2021*, pages 29–35, 2021.

[9] Priyanka Nanayakkara, Johes Bater, Xi He, Jessica Hullman, and Jennie Rogers. Visualizing privacy-utility trade-offs in differentially private data releases. *arXiv preprint arXiv:2201.05964*, 2022.

[10] Johnny Saldaña. *The coding manual for qualitative researchers*. sage, 2021.

[11] Aiping Xiong, Tianhao Wang, Ninghui Li, and Somesh Jha. Towards effective differential privacy communication for users' data sharing decision and comprehension. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 392–410. IEEE, 2020.

[12] Aiping Xiong, Chuhao Wu, Tianhao Wang, Robert W Proctor, Jeremiah Blocki, Ninghui Li, and Somesh Jha. Using illustrations to communicate differential privacy trust models: An investigation of users' comprehension, perception, and data sharing decision. *arXiv preprint arXiv:2202.10014*, 2022.