Usability Testing Plan and Educational Documents for Differential Privacy

Jack Landry
Mentors: Mark Bun, Dan Muise, Kobbi Nissim, Elizabeth Quigley

Part of the Privacy Tools Project at Harvard University

November 29, 2016

1 Task and Context

Prior to this summer, the privacy tools team has focused its efforts on the private data sharing interface tool (PSI). However, very little work has been done preparing PSI for use among researchers without prior knowledge of differential privacy. My project fills this gap. To educate researchers who have no background in differential privacy, I created short educational documents that give all the necessary background information needed to use PSI. To ensure that the PSI tool is as user friendly as possible, I created a usability testing plan that will contribute to the development and the eventual public release of PSI.

2 Main Principles and Goals

2.1 Principles

All components of my project this summer were designed foremost for the needs of first time users of PSI and differential privacy.

2.2 Goals

1. **The creation of educational documents for each persona in the PSI system (data depositors and data analysts).** These documents were kept as short and nontechnical as possible to ease the barriers to using PSI.

2. **The create of a usability testing plan for PSI** This test was designed to be as realistic as possible, mimicking researchers' actual use of PSI.

3 Contributions

3.1 Educational Documents

At the PSI tool gets closer to public release, it's essential that first time users have educational materials that explain how to use it. Statistical analysis via differential privacy includes many novel components, such as the epsilon privacy budget, accuracy parameters, added noise, bounded queries, and restricted assess to raw data. To successfully use differential privacy and the PSI system, users need to be guided though how to deal with these novel components. To that end, my project created short educational documents that give detailed guidance on how to use differential privacy and PSI.

3.1.1 Preexisting Educational Documents

There have been several educational documents developed by the Privacy Tools team before my project.

- **PSI paper** Gives a technical explanation of differential privacy and the PSI system but is intended for a technical computer science audience, not social scientists.
- **Social Science Paper** Gives a comprehensive overview on both the failures of de-identification and how differential privacy works but does not provide guidance on how to use PSI or how to interpret differentially private statistics.
- **Differential Privacy in CDFs Slides** Gives a comprehensive overview of how to interpret differentially private statistics, but is intended only for data analysts and is very long.

All of these documents are quite long and do not give detailed instructions on how to deposit and analyze data with differential privacy. My project created educational documents that fill this gap. Specifically, I created three short educational documents tailored to potential users of differential privacy.

3.1.2 Newly Created Educational Documents

The following three educational documents provide short and focused text explaining both why researchers would want to use differential privacy as well as how to use it.

- **Overview** Introduces the problems with assessing sensitive datasets and how differential privacy helps to solve these problems. Gives a broad overview of how differential privacy protects individuals from identification.
- **How to Analyze Data with Differential Privacy** Gives a short yet comprehensive explanation of how to analyze data with differential privacy. Introduces privacy budget and accuracy parameter.
- **How to Deposit Data with Differential Privacy** Gives a brief explanation of how to make sensitive data available for exploration with differential privacy. Requires further development to provide guidance about legal issues.

3.2 Usability test

My design of a usability testing plan for the PSI tool will inform its development for future non-expert users. Thus far, the development of PSI has been geared toward basic functionality and improving the accuracy of differentially private algorithms. There has also been a lot of work done on software development, interrogating differential privacy with Dataverse, TwoRavens, and Zelig. My work creating a usability test will build on all these elements–ensuring that they work well for actual users. When the usability test is actually preformed, its results will inform the further development of the tool.

3.3 IRB Approval of Usability Test

To carry out the usability test, it requires need to be approved by the Harvard Institutional Review Board. To that end, I completed an application to the Harvard IRB usability testing plan. After review and approval by the Harvard IRB, the usability test will be ready to carry out.

4 Results, Summary, and Points for Future Research

4.1 Results of Educational Documents

Originally, only two educational documents were planned; an overview of how to deposit data with differential privacy as well as an overview of how to analyze data with differential privacy. As the project wore on, it became clear that another short document that provided a broad overview of differential privacy was logical addition to the broad goal of educating users about differential privacy. The overview document provides a brief explanation of what differential privacy is and how it protects privacy. It could stand on its own or attach to the how to analyze and how to deposit documents.

4.1.1 Overview

As described above, the overview document provides brief background on what differential privacy is and how it protects privacy. Importantly, it starts with social scientists background for how differential privacy can be useful. It explains how an increasingly large number of datasets are restricted in access and how differential privacy allows researchers to make an informed decision on whether to apply for full access.

After explaining the motivation for use of differential privacy, the overview briefly mentions the privacy preserving mechanisms of differential privacy. Immediately after explaining each privacy preserving mechanism (no access to raw data, limited queries and insertion of noise) the document explains why each are necessary to protect privacy.

Throughout the creation of these documents, it was difficult to strike a balance between informing users of the novel and utility reducing components of differential privacy without making it seem that differential privacy is too limited to be useful. There are two schools of thought on this issue. In my view, as long as users understand that differential privacy is opening up assess to data that was previously restricted, there is no need to downplay the utility reducing features of differential privacy. However, this option was scuttled since the utility reducing features of differential privacy are so unique and unsettling. You can refer to the final draft of the current analyzer document to see exactly how these features are introduced.

At one point during the course of the project, this overview also provided information on how de-identification was insufficient in protecting privacy. Although this part has been omitted from the correct draft of the document, the text is available for use elsewhere.

Importantly, the overview text can both stand on its own or be attached to the texts of the analyzer and depositor documents. If the overview stands alone, it gives background on why differential privacy is useful and an overview of how it protects privacy. This type of documents is important for those interested in learning about differential privacy without a specific plan on how to use it. The depositor and analyzer documents give more detailed instructions on how to use differential privacy that isn't necessary for those that are looking for a minimal conceptual understanding.

4.1.2 How to Analyze Data With Differential Privacy

This document gives detailed instructions on how to analyze sensitive datasets with differential privacy. It starts by explaining the privacy budget epsilon. The key points are that the depletion of epsilon is additive, that higher levels of epsilon increases accuracy. It also points out that deferentially private statistics will generally be more accurate for higher sample sizes n. There is text both types of implementations of differential privacy, where epsilon is allotted to each user of the dataset (trusted not to collaborate version) and epsilon is allotted for the dataset and each user takes away from the global budget. In the future this text may need to be updates as one of these versions may not be feasible due to ongoing legal issues.

Besides the allocation of epsilon, the analyzer documents also provides guidance on how users can select for the accuracy of their statistics. It explains that users can input a given accuracy level and find how much epsilon that query would take. It provides the general guidance that data analysts should select the minimal level of accuracy they need to minimize their epsilon depletion.

A guiding principle in creating all the educational documents was to make them as short a reader friendly as possible. To that and, in an effort to break up the text, a flowchart was added. The flowchart illustrates how deferentially private statistics are calculated behind the scenes. In an interactive query tool where analysts don't have access to the data, it's important to demonstrate how statistics are calculated when you aren't calculating them yourself.

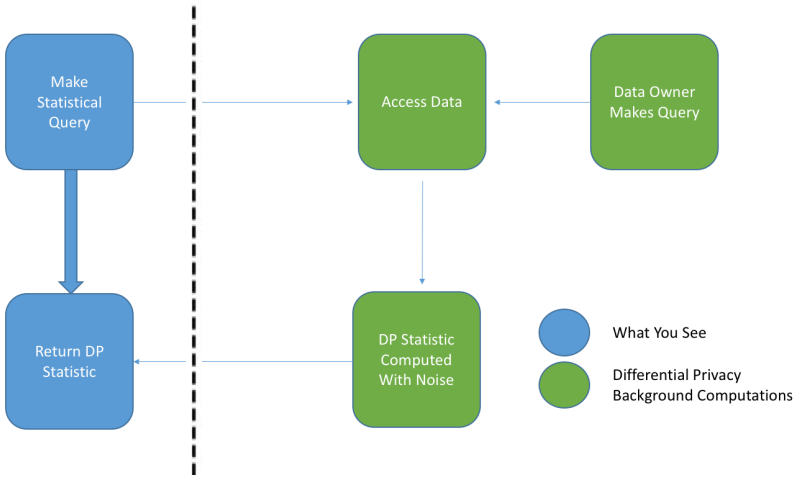

Figure 1: Analyst Flowchart

4.1.3 How to Deposit Data with Differential Privacy

This document gives detailed instructions on how to deposit data so others can assess it via differential privacy. There are a few different possible scenarios for which the depositor can provide sensitive data for assess with the PSI system. The depositor document gives guidance on each of these scenarios in turn.

In one scenario, the depositor releases statistics for data analysts but does not allow the data analysts to do any interactive queries. The only deferentially private statistics that are available to data analysts would be those that are released by the depositor. This scenario might be common in cases where the allowed use of the sensitive data is limited. For instance, as part of a data usage agreement, the owner may be barred from exploring the relationship between certain variables. In this case, it's emphasized that data owners should release as many broad statistics from the data as possible to give analysts a good idea of its usefulness. Since analysts cannot perform queries themselves, depositors need to anticipate their needs as much as possible.

In the second scenario, depositors release some statistics to analyzers at the time of deposit but preserve some of the epsilon privacy budget to allow data analysts to make interactive queries. This is likely to be the most common scenario. In this situation, depositors must try to strike a balance between releasing broadly useful statistics themselves while preserving enough privacy budget for data analysts. By releasing broadly useful statistics, depositors give data analysts initial information about the usefulness of the dataset. From there, data analysts an make their own very specific queries to see if the data confirms to their specifications.

In the last scenario, data depositors don't release any statistics, preserving the entire privacy budget for data analysts. Data analysts perform all the queries and have no access to initially pre-released statistics. This scenario is the least burdensome on data depositors. They don't need to go though the process of querying for statistics, all they need to do is allocate a privacy budget for users. In this case, it may not be necessary for depositors to understand the details of how querying for statistics works in the PSI system. While this information should be made available to them, all that's absolutely necessary is information about what level of epsilon is acceptable for the type of data they're releasing.

Similar to the problems explaining PSI to the analyzer, data depositors may be confused at how differential privacy computes statistics with the raw data. In the interest of readability, the computations are explained via a flowchart, shown in figure 2. The flowchart breaks up the text and illustrates the workflow rather than explaining it with words.

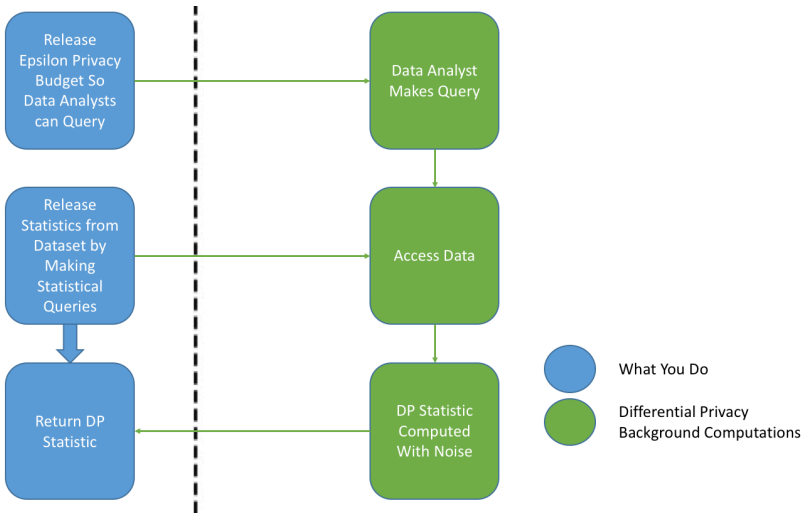

Figure 2: Depositer Flowchart

4.2 Results of Usability Testing Plan

The usability testing plan presents a way to comprehensively evaluate the PSI system. For users to successfully use PSI, they must have both a conceptual understanding of differential privacy as well as a technical competency with the system. For instance, if a user is struggling allocating epsilon between different statistics, it may be because the button the budgeting tool is in the wrong place. Alternatively, it could be that the educational documents do a poor drop explaining how epsilon allocation works. In the first scenario, the failure has to do with the technical design of the system. But the second scenario, the failure is educational. Since both of these failures are possible, the usability testing plan must evaluate both the usability of the PSI system (for technical failures) as well as the success of the associated educational documents.

Before the body of the usability test, there is a section of questions that assess use cases and participants background dealing with private, confidential data. It's meant to gather information on ensuring that PSI's use cases integrate with researchers' work flow. Questions about how researchers work with sensitive data are meant to better tailor the motivational section of the educational document to ensure that everything that's described is true to researchers experiences. There answers will help tailor the motivational section of the overview document. Furthermore, learning about how social scientists access sensitive research data could help inform use cases beyond what's currently been envisioned by the privacy tools team.

After discussion with the (now departed) user experience exert in IQSS Elizabeth Quigley, it was decided that questions about user experience should be staggered throughout the reading of the educational documents. The reasoning behind this decision was to maximize engagement of participants. Instead of awkwardly watching participants silently read a document for several minutes, successive paragraphs will be broken up with questions regarding those paragraphs. These questions are mostly directed at users reactions to the reading, making sure that everything makes sense, that the PSI tool seems relevant to their research, and that the document is comprehensive enough to leave them without important outstanding questions.

After reading the educational documents, participants will answer more comprehensive usability test questions. These will require users to integrate all their knowledge from the previous reading. Questions will test users understanding about epsilon allocation, accuracy, sources of noise, delta, and other points that are integral to the proper use of the PSI system. Eventually, these questions should ask participants to do different tasks in the PSI system, covered in the future work section of this paper.

4.2.1 Results of IRB Application

The Internal Review Board Application has been completed at much as possible before the testing plan is finalized. The only remaining parts of the usability testing plan concern minor technicalities that are yet to be decided upon. For instance, it's still to be determined if there will be any personnel not affiliated with Harvard working on the project, which would require a separate form. The specific details of what needs to be completed is included in the future work section of this document.

The usability test IRB application is considered "non-exempt" since it deals with human subjects. (Even exempt research needs to be reviewed by the IRB to confirm its exempt status.) The application details the specific procedures of the usability test, including consent, compensation, storage of data, and recruitment of subjects.

4.3 Future Work

4.3.1 Integration with PSI

The most important future task for revising the usability test and educational documents is further integration with the PSI system. During my project, the development of the PSI tool was still in progress. Since the user interface and work-flow was changing dramatically, tailoring the educational documents and usability test for the PSI tool was a challenge. As the PSI tool is finalized, these items should be fully integrated with the system.

The goal of both the usability testing plan and the educational documents is to ensure the easy use of the PSI system. Currently, all of these documents speak more generally to the concept of differential privacy. While a basic conceptual understanding of differential privacy is essential to understand the system, more specific guidance is necessary to make the PSI system easy to use.

Educational Documents As aspects of the PSI tool are finalized, the educational documents should be made to specifically reference the tool. For instance, instead of speaking generally about selecting an epsilon, the documents should make reference to where you'd select epsilon on the PSI interface. Screenshots and other images should be created to further guide users though how to use the tool.

Usability Test The usability test needs the most revision to make it specific for the PSI system. The usability test should be performed with the actual PSI system, not by answering questions on pen and paper. That requires new questions that use real data and queries on the PSI system.

4.3.2 IRB Approval of Usability Test

The second most important future task for this project is getting the usability test approved by the Harvard IRB. To that end, some sections of the IRB application for the PSI usability evaluation still need to be completed, contingent on finalizing the procedures of the test and who will be involved.

- If non-Harvard personnel participate in administering the study, a separate forum will need to be filled out.
- If there is a plan to share the results of the study outside of the research team, the specifics of the sharing will need to be described.
- After a PI (Primary investigator) is chosen, a section will need to be filled out describing, "the experience of the investigator with the proposed research procedures and population."
- The plan or compensation needs to be finalized and included in the application materials. Currently, the plan is to present participants with a 10 dollar Amazon gift card, but that should be confirmed.

4.3.3 Depositing Data with Differential Privacy

While all current educational documents are drafts, the depositor document is the most unfinished due to outstanding issues about how depositing data will actually work. The most important outstanding

issue is giving guidance about epsilon allocation. The current paradigm of data privacy in the social sciences thinks of privacy as binary, data is either entirely protected and confidential protected or totally open to the public. Epsilon explicitly acknowledges privacy loss from every statistical computation, and thus requires a more enlightened understanding of privacy that is continuous instead of dichotomous.

This new understanding of privacy has to be integrated with existing privacy laws. Different types of data have different laws associated with them with potentially different implications for differential privacy. These come at the state, national, and international level. There will also need to be guidance on dealing with researchers' institutional review boards.

At this point, differential privacy has not been confirmed to be legal to use for any types of sensitive data. However, legal research in this area are ongoing and regulations are periodically updated. When more information concerning the legality of differential privacy becomes available, it should be integrated into the depositor document. There is a potential collaboration between the PSI tool and legal tagging software being developed for the Harvard Dataverse that would ease the process for depositors and prevent them answering repetitive questions.

Exactly what integrating the guidance for data depositors with legal research means is dependent on the outcomes of the legal team's work. However, it's thought now that different types of sensitive data would have different types of associated epsilon budgets. More sensitive data would get a smaller global epsilon budget as privacy leakage would be more damaging. Extending this guidance and making it more specific should be one of the most important tasks for future work.

4.3.4 Depositing Data with Differential Privacy that Has Already Available in De-Identified Form

Legal issues surrounding differential privacy are very complicated and presumably will require a considerable amount of time to be resolved. One possible area differential privacy could be implemented while avoiding legal issues is upgrading the protection of currently publicly available, de-identified data. In the past, de-identified data has been repeatedly been shown to be vulnerable to de-identification attacks. Therefore, it follows that currently de-identified data could be vulnerable to the same types of attacks that identify individuals private information. Differential privacy could be applied to currently de-identified datasets, keeping the anonymization and applying the differential privacy process to provide additional privacy protection. Since this privacy guarantee is stronger than de-identification and de-identification has already been judged to comply with privacy laws and regulation, the addition of differential privacy seemingly avoids any knotty legal issues. As the PSI tool readies public release yet legal issues remain unresolved, depositing already publicly released anatomized data with differential privacy could be a preliminary use for PSI. If this is possible, specific guidance for depositors in this situation should be crafted.

4.3.5 PSI Demo Tool

When new users query for statistics in PSI, they operate in a high stakes environment. Every query utilizes some of the epsilon privacy budget. If a new user that just learning to use the system accidentally uses his whole privacy budget for a mean of one variable, there's no undo button. While this issue makes user education and usability testing all the more important, it could also be ameliorated by creating part of PSI to demo.

A PSI demo could take several forms. In the simplest version, the new user would work with non-sensitive, perhaps the California PUMS dataset that has already been a part of various demos of PSI. The PSI tool could be slightly recoded to make the epsilon privacy budget replenishable. In an even simpler form, the allocated epsilon privacy budget could be set to a very high number, allowing a user to play around with queries without worrying about getting locked out. However, this would not be optimal for illustrating the limited queries associated with a given privacy budget.

More complicated demo tools would require more coding but would also be more effective.

4.3.6 Separate Educational/Promotional Document: Why Differential Privacy is Useful

After reviewing educational documents of other statistical query systems, it may make sense to create a very short document explaining how differential privacy can be useful to social scientists. This would be very short and non-specific, intended only to "sell" social scientists of the concept of differential privacy. While explaining PSI's basic functionality, this document would refrain from delving into any technical details.

The goal of this document would be to solely explain how differential privacy could be used by social scientists, motivating researchers to learn more. Researches would not come upon this document already intending to use PSI or seeing some potential for its use. (For these situations the more comprehensive overview document is more appropriate) Rather, this document would help popularize differential privacy in the social scientists by raising awareness of its usefulness, motivating social scientists to look for how it could be used in their own work themselves.