Effect of Facts Box on Users' Comprehension of Differential Privacy: A Preliminary Study

Aiping Xiong[1], Tianhao Wang[2], Ninghui Li[2], Somesh Jha[3]
[1]The Pennyslvina State University, [2]Purdue University, [3]University of Wisconsin-Madison

In the context of data release, differential privacy (DP) has been proposed to protect individuals' data privacy and ensure utility (Dwork, 2006). Specifically, DP adding noise to aggregated results such that the difference of whether or not an individual is included in the data is bounded. DP techniques are currently being transitioned from academic to industry, e.g., the US Census Bureau has deployed DP technologies for the 2020 census (Abowd, 2018). One interesting and important open question is whether users understand these techniques, trust their protection, and consequently increase their data disclosure when these techniques are deployed (Xiong, Wang, Li, & Jha, 2020).

In DP models, the random noise introduced to protect individual privacy also affects the accuracy of statistical analysis, especially for small- or moderately-sized datasets. Thus, a communication on privacy-utility tradeoff, i.e., obtaining the maximum possible utility while preserving differential privacy, is important to help people make informed data-participation decisions. Schwartz, Woloshin, and Welch (2009) proposed the facts box to communicate evidence based on benefits and harms of medication and obtained results showing that drug facts box improved consumers' understanding of the benefit and side effects. The facts box has also been used to help people make informed decision on medical health screening (McDowell, Rebitschek, Gigerenzer, & Wegwarth, 2016).

The present study is a preliminary work investigating the effect of facts box to communication benefits, costs, and compromise risks of the DP technique to users. Using a between-subject design, we evaluated the effect of facts box with three visual presentations, one using barchart and the other two using dotplot. In the barchart condition, injected random noise was presented as the difference of bar heights. In the dotplot and dotplot background conditions, number of dots was used to present added random noise. The two conditions were the same except that the compromised users became transparent dots but still visible in the dotplot background condition. We conducted an online human-subject experiment on Amazon Mechanical Turk. Within a health-app data collection setting, participants were informed of re-identification issue of anonymous aggregated data. After viewing one version of the facts box, participants made one data-participation decision for sensitive personal information (e.g., family medical record) and then indicated the reasons why they made the decision. Participants then rated 1) whether the facts box was helpful for them to understand DP and 2) the trustworthiness of the described DP technique. We also evaluated participants' objective comprehension of DP with four questions.

Participants' data-participation rates were slightly better than chance and showed no difference across conditions. For each condition, about 80% of the participants indicated that the facts box was helpful for them to understand DP but the average correct answer rate for the objective comprehension questions was only about 40%, revealing that participants had difficulty in understanding privacy and utility implications of DP. Trustworthiness rating of the dotplot background condition tended to be better than the other two conditions. We did thematic analysis for the answers to why participants made the share or not share decisions. For participants who chose to share, the top two themes were the descriptions of DP (30%) and utility concern for participants themselves and others (21%). For participants who chose not to share, the top theme was their worrisome of data compromise and non-deletion (69.5%). The second theme was that the health information was too sensitive to share (18.3%).

Acknowledgments. This work was partly supported by the NSF awards #1640374 and #1931443.

References

1. Abowd, J. M. (2018). Protecting the confidentiality of America's statistics: Adopting modern disclosure avoidance methods at the census bureau. Retrieved from https://www.census.gov/newsroom/blogs/research-matters/2018/08/protecting_the_confi.html.
2. Dwork, C. (2006). Differential privacy. In *ICALP*, pp. 1–12.
3. McDowell, M., Rebitschek, F. G., Gigerenzer, G., and Wegwarth, O. (2016). A simple tool for communicating the benefits and harms of health interventions: a guide for creating a fact box. *MDM Policy & Practice*, *1*(1):2381468316665365.
4. Schwartz, L. M., Woloshin, S., and Welch, H. G. (2009). Using a drug facts box to communicate drug benefits and harms: two randomized trials. *Annals of Internal Medicine*, *150*(8): 516–527.
5. Xiong, A., Wang, T., Li, N., & Jha, S. (2020). Towards Effective Differential Privacy Communication for Users' Data Sharing Decision and Comprehension. In *Proceedings of the 41st IEEE Symposium on Security & Privacy*. Digital Conference.