Communicating the Privacy Functionality of PETs to eHealth Stakeholders

ALA SARAH ALAQRA, FARZANEH KAREGAR, and SIMONE FISCHER-HÜBNER, Karlstad University, Sweden

In the EU H2020 PAPAYA project, a PlAtform for PrivAcY-preserving data Analytics, which can run in an untrusted Cloud environment, was developed and demonstrated for medical use cases. A first use case involved the data analysis on homomorphically encrypted ECG signal data of patients on the PAPAYA platform [1], and a second use case involved differential privacy (DP) for collaborative learning on medical data [3]. For fostering trust and providing usable transparency for eHealth stakeholders, we conducted user studies in the form of interviews with eHealth professionals (first use case) and with individuals in the data subject role (second use case). As these revealed, providing transparency of privacy-enhancing technologies (PETs) in a usable manner poses several challenges. Communicating different privacy and security features of PETs, including their capability of guaranteeing both data minimisation and data quality for assuring patient safety, is of key importance [1]. Our studies revealed misconceptions that participants had where they may have assumed that a PET, such as homomorphic encryption or DP, would be functioning in a similar way as technologies they are familiar with (commonly in-use security technologies such as encryption) [1, 3]. Commonly used metaphors (e.g., pixelation of photos used for DP) may also rather provide a structural explanation for a PET, while recent research has shown that functional explanations of privacy and security technologies are better understandable for end users [2]. A better understanding of functional explanations by both expert and lay users was also confirmed by the results of our ongoing work, while structural explanations were perceived as more trustworthy. Therefore, higher emphasis should be put on functional explanations of PETs (while further structural explanations may be needed for fostering reliable trust in the PETs). Particularly, approaches for providing usable functional explanations on how PETs can adequately reduce privacy risks while maintaining data quality for assuring patient safety need further research. Communicating this information could also be supported by the results of a conducted Privacy Impact Assessment (PIA). Our interviews with eHealth professionals showed such information and already just the fact that a PIA was conducted was appreciated and increased trust in the PET [1]. Still, participants requested further information about the PIA method and how it was conducted, the qualification of the individuals that conducted the PIA, as well as the PET method [1] (incl. structural information on how Homomorphic Encryption works - confirming the relevance of additional structural explanations). Based on our research, this workshop paper aims to contribute to the discussion of usable explanations of PETs for eHealth stakeholders, how to address challenges and future research directions.

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).

ACM Reference Format:
Ala Sarah Alaqra, Farzaneh Karegar, and Simone Fischer-Hübner. 2023. Communicating the Privacy Functionality of PETs to eHealth Stakeholders. In *ACM CHI'23 workshop*. ACM, New York, NY, USA, 2 pages. https://doi.org/XXXXXXX.XXXXXXX

REFERENCES

[1] 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.

[2] 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.

[3] Farzaneh Karegar, Ala Sarah Alaqra, and Simone Fischer-Hübner. 2022. Exploring {User-Suitable} Metaphors for Differentially Private Data Analyses. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. 175–193.

Received February 2023; revised XXX ; accepted XXX