

Current Topics in Inverse Transparency

Thesis or Guided Research

Supervisor: Prof. Dr. Alexander Pretschner

Advisor: Valentin Zieglmeier

Email: zieglmev@cit.tum.de

Phone: +49 (89) 289 - 17834

Starting date: flexible

Informatics 4 – Chair of Software and Systems Engineering
Prof. Dr. Alexander Pretschner

TUM School of Computation,
Information and Technology
Technical University of Munich

Boltzmannstr. 3 (5611)/I
85748 Garching b. München

<https://www.cs.cit.tum.de/en/sse/>

Context

In an increasingly digitalized world, individuals depend on technical systems that process their data. Everything from human resources to voter registrations is now handled by computer systems, which means that data are utilized. Individuals lack oversight over these systems, which can lead to discrimination and hidden biases that are hard to uncover. Recent data protection legislation tries to tackle these issues, but it is inadequate.

The research project “Inverse Transparency” tries to improve upon existing data protection by giving data owners more sovereignty in how their data are used. Its core idea is to enable access to data on a more case-by-case basis, but to monitor all accesses and make them transparent to data owners. On the one hand, this can help to raise awareness of data usages and better protect the employee’s personal data, on the other hand it may enable usages of data useful to teams and individuals alike.

Potential topics

Various research problems arise. First, this covers more technical problems in the area of secure logging (integrity protection, confidentiality measures, performance issues) with technologies such as Intel SGX or blockchain-based logs. Second, the human-computer interaction aspects are considered, with questions concerning usability and trustworthiness (understandability, ease of use, personalization, perceived reliability) being addressed. Third, the question of giving meaning to Inverse Transparency is relevant, on the one hand covering privacy-preserving analytics, and on the other hand addressing data owners’ motivation to share.

It can be instructive to look at past topics that have been completed under my guidance (see [here](#)), but these are meant as an inspiration, not a limitation.

Relevant previous experience

Participation in [my seminar](#) or [practicum](#) is considered a plus, but not required. Any other course covering relevant knowledge for the topic area you are interested in is beneficial. Apart from that, completion of at least one seminar course (or equivalent) is required.

Application

Please read our publications on the topic of Inverse Transparency [1, 2]. If you have a concrete research direction or topic in mind, additional reading in that area is a plus. Suggestions for reading are provided below [3–8].

Apply [via email](#) and include your relevant previous experience (see above), your topic interests, and your preferred timeline.

References

- [1] Zieglmeier, Valentin, and Alexander Pretschner (2021). “Trustworthy Transparency by Design.” arXiv preprint arXiv:2103.10769. Available: <https://arxiv.org/pdf/2103.10769>
- [2] Zieglmeier, Valentin, and Gabriel Loyola Daiqui (2021). “GDPR-Compliant Use of Blockchain for Secure Usage Logs.” In EASE 2021: Evaluation and Assessment in Software Engineering, ACM (pp. 313–320). Available: <https://arxiv.org/abs/2104.09971>
- [3] Agrawal, Rakesh et al. (2002). “Hippocratic databases.” In VLDB’02: Proceedings of the 28th International Conference on Very Large Databases (pp. 143–154). Available: <http://agrawal-family.com/rakesh/papers/vldb02hippocratic.pdf>
- [4] Farke, Florian M. et al. (2021). “Are Privacy Dashboards Good for End Users? Evaluating User Perceptions and Reactions to Google’s My Activity.” In USENIX Security 21: 30th USENIX Security Symposium (pp. 483–500). Available: <https://www.usenix.org/system/files/sec21-farke.pdf>

- [5] Chellappa, Ramnath K. (2008). "Consumers' trust in electronic commerce transactions: the role of perceived privacy and perceived security." Unpublished manuscript, Emory University, Atlanta, GA. Available: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.113.8730&rep=rep1&type=pdf>
- [6] Bruno Lepri et al. (2018). "Fair, transparent, and accountable algorithmic decision-making processes." In *Philosophy & Technology* 31.4 (pp. 611–627). Available: <https://link.springer.com/article/10.1007/s13347-017-0279-x>
- [7] Birrell, Eleanor, et al. (2018). "SGX enforcement of use-based privacy." In WPES 2018: Proceedings of the 2018 Workshop on Privacy in the Electronic Society. Available: <https://www.cs.cornell.edu/fbs/publications/UBP.SGX.pdf>
- [8] Zyskind, Guy et al. (2015). "Decentralizing privacy: Using blockchain to protect personal data." In 2015 IEEE Security and Privacy Workshops (pp. 180–184). Available: <https://web.media.mit.edu/~guyzys/data/ZNP15.pdf>

Informatics 4 – Chair of Software and Systems Engineering
Prof. Dr. Alexander Pretschner

TUM School of Computation,
Information and Technology
Technical University of Munich

Boltzmannstr. 3 (5611)/
85748 Garching b. München

<https://www.cs.cit.tum.de/en/sse/>