EGU2020-13071
https://doi.org/10.5194/egusphere-egu2020-13071
EGU General Assembly 2020

The Dark Side of the Knowledge Graph - How Can We Make Knowledge Graphs Trustworthy?

Robert Huber[1] and Jens Klump[2]
[1]MARUM - Center for Marine Environmental Sciences, University of Bremen, Bremen, Germany
[2]Mineral Resources, CSIRO, Kensington WA, Australia

"*We kill people based on metadata.*" (Gen. Michael V. Hayden, 2014) [1]

Over the past fifteen years, a number of persistent identifier (PID) systems have been built to help identify the stakeholders and their outputs in the research process and scholarly communication. Transparency is a fundamental principle of science, but this principle of transparency can be in conflict with the principles of the right to privacy. The development of Knowledge Graphs (KG), however, introduces completely new, and possibly unintended uses of publication metadata that require critical discussion. In particular, when personal data, as is linked with ORCID identifiers, are used and linked with research artefacts and personal information, KGs allow identifying personal as well as collaborative networks of individuals. This ability to analyse KGs may be used in a harmful way. It is a sad fact that in some countries, personal relationships or research in certain subject areas can lead to discrimination, persecution or prison. We must, therefore, become aware of the risks and responsibilities that come with networked data in KGs.

The trustworthiness of PID systems and KGs has so far been discussed in technical and organisational terms. The inclusion of personal data requires a new definition of 'trust' in the context of PID systems and Knowledge Graphs which should also include ethical aspects and consider the principles of the General Data Protection Regulation.

New, trustworthy technological approaches are required to ensure proper maintenance of privacy. As a prerequisite, the level of interoperability between PID needs to be enhanced. Further, new methods and protocols need to be defined which enable secure and prompt cascading update or delete actions of personal data between PID systems as well as knowledge graphs.

Finally, new trustworthiness criteria must be defined which allow the identification of trusted clients for the exchange of personal data instead of the currently practised open data policy which can be in conflict with legislation protecting privacy and personal data.

[1] https://www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/